



**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**MÔN THỰC TẬP CƠ SỞ**



**BÀI THỰC HÀNH 2.1**  
**Cài đặt, cấu hình mạng doanh nghiệp với Pfsense Firewall**

**Tên sinh viên: Nguyễn Văn Hùng**

**Mã sinh viên: B22DCAT136**

**Nhóm: 09**

**HÀ NỘI, THÁNG 03/2025**

## MỤC LỤC

MỤC LỤC .....	1
DANH MỤC CÁC HÌNH VẼ .....	2
I. GIỚI THIỆU CHUNG .....	4
1. Mục đích .....	4
2. Lý thuyết .....	4
2.1. Switch ảo (Virtual Switch) .....	4
2.2. Card mạng ảo (Virtual Network Adapter) .....	6
2.3. DHCP Server ảo (Virtual DHCP Server) .....	6
2.4. Thiết bị NAT .....	8
2.5. Cấu hình kết nối mạng .....	8
I. NỘI DUNG THỰC HÀNH .....	10
1. Chuẩn bị môi trường .....	10
2. Thực hành .....	10
2.1. Cấu hình topo mạng .....	10
2.2. Cài đặt cấu hình pfSense firewall cho lưu lượng ICMP .....	15
2.3. Cài đặt cấu hình pfSense firewall cho phép chuyển hướng lưu lượng tới21	
TÀI LIỆU THAM KHẢO .....	25

## DANH MỤC CÁC HÌNH VẼ

Hình 1. Virtual Network Editor trên VMware pro 17 .....	4
Hình 2. Card mạng tương ứng trên máy thật .....	5
Hình 3. Card mạng ảo kết nối máy thật .....	6
Hình 4. Virtual Network Adapter .....	6
Hình 5. Virtual DHCP Service .....	7
Hình 6. DHCP Settings .....	7
Hình 7. Bridged mode .....	8
Hình 8. NAT mode .....	8
Hình 9. Host-only mode .....	9
Hình 10. Topo mạng cần chuẩn bị .....	10
Hình 11. Máy Kali Linux attack 1 .....	11
Hình 12. Máy Windows attack .....	11
Hình 13. Ubuntu Linux victim .....	11
Hình 14. Windows Server victim .....	12
Hình 16. Máy Windows Server 2019 victim .....	12
Hình 17. Cấu hình pfSense .....	13
Hình 18. Kết nối Kali Linux Attack (Internal) và pfSense LAN .....	13
Hình 19. Kết nối từ Windows attack đến Kali Linux Attack 1 (Internal) .....	14
Hình 20. Kết nối Windows Server Victim (External) và pfSense WAN .....	14
Hình 21. Kết nối Windows Server Victim và Kali Linux Attack 2 (External) ....	15
Hình 22. Đăng nhập pfSense .....	15
Hình 23. Giao diện pfSense .....	16
Hình 24. Cấu hình cho phép ICMP từ Internal ra External .....	16
Hình 25. Lưu thay đổi LAN .....	17
Hình 26. Chặn ICMP từ External vào Internal .....	18
Hình 27. Chặn ICMP từ External vào Internal .....	18
Hình 28. Lưu thay đổi WAN .....	19
Hình 29. Kiểm tra ping từ Internal ra ngoài .....	19
Hình 30. Kiểm tra chặn ping từ External vào Internal .....	20

Hình 31. Kiểm tra cổng TCP .....	20
Hình 32. Cấu hình Port Forwarding .....	21
Hình 33. Apply Changes Port Forward .....	22
Hình 34. SSH đến địa chỉ IP tường lửa pfSense .....	23
Hình 35. Kiểm tra IP .....	23
Hình 36. Kiểm tra cổng .....	23

# I. GIỚI THIỆU CHUNG

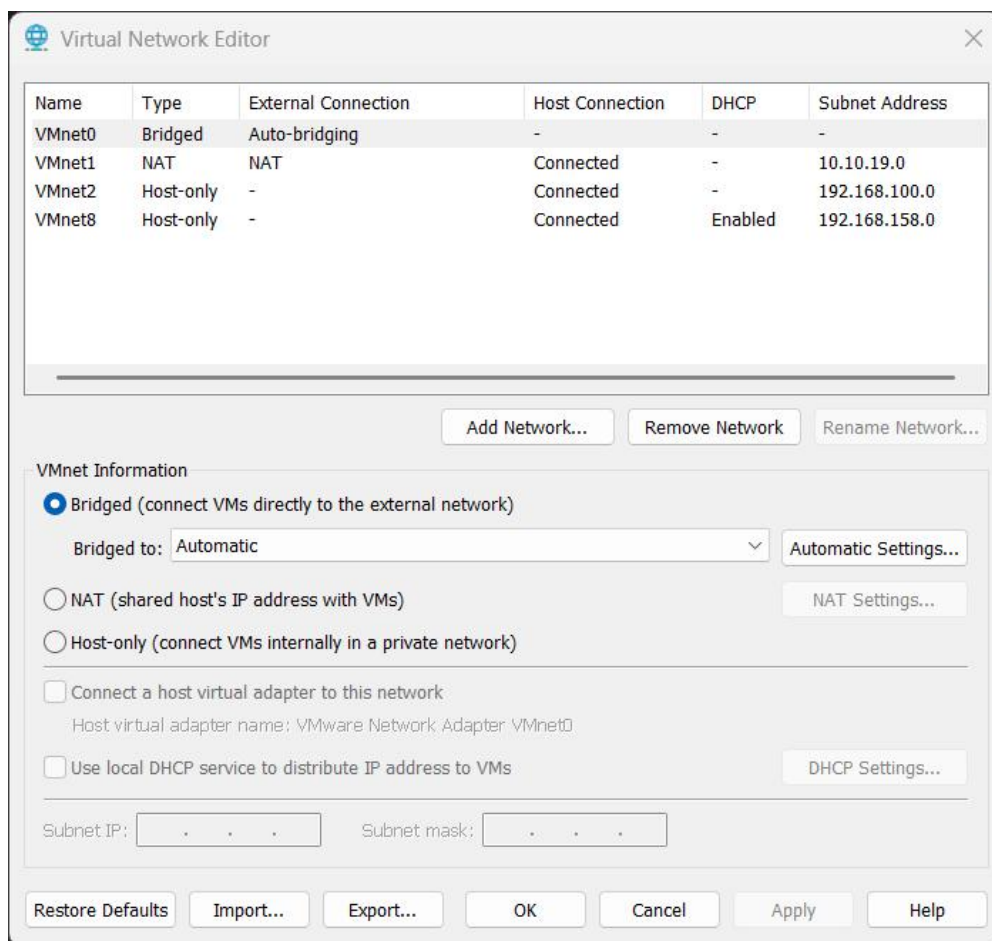
## 1. Mục đích

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. Lý thuyết

Để cấu hình mạng ảo của VMware, ta chọn trên thanh menu: **Edit → Virtual Network Editor...**



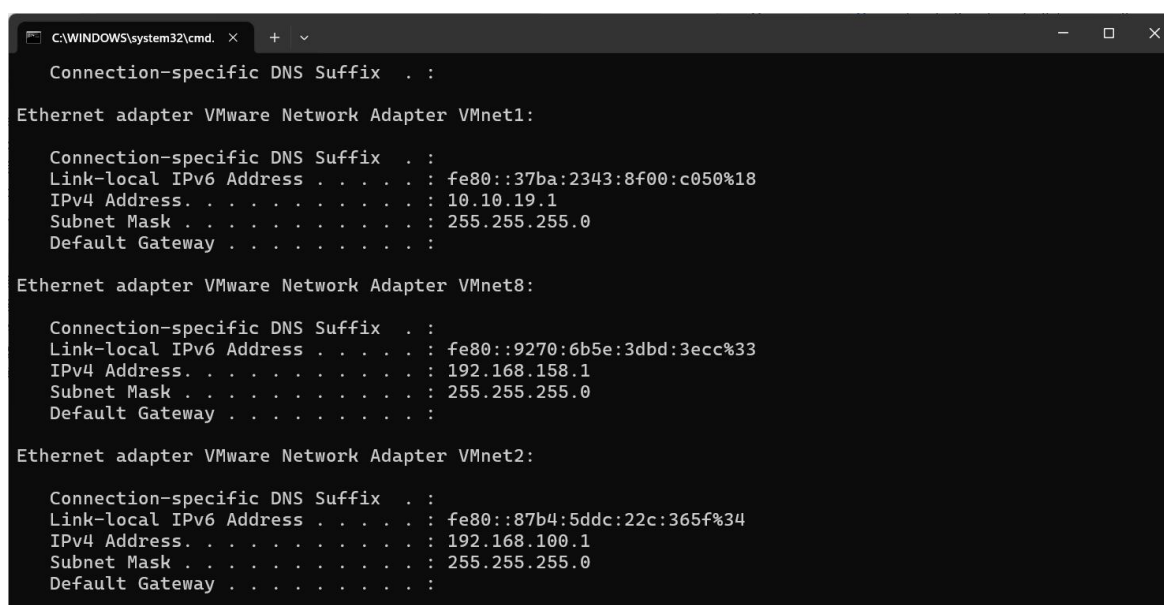
Hình 1. Virtual Network Editor trên VMware pro 17

### 2.1. Switch ảo (Virtual Switch)

Đóng vai trò như một bộ chuyển mạch ảo, giúp kết nối các máy ảo với nhau hoặc với mạng bên ngoài. Những switch ảo hay còn gọi là mạng ảo, chúng có tên là VMnet0, VMnet1, VMnet2... một số switch ảo được gắn vào mạng một cách mặc định. Mặc định khi ta cài VMware thì có sẵn 3 Switch ảo: VMnet0 chế độ Bridged, VMnet8 chế độ NAT và VMnet1 chế độ Host-only.

VMware Workstation (pro 17) cho phép tạo 20 switch ảo. Mỗi Switch ảo kết nối không có giới hạn cụ thể số lượng máy ảo, chủ yếu phụ thuộc vào tài nguyên hệ thống của bạn (CPU, RAM, băng thông), với Host-Only và NAT có thể bị giới hạn bởi DHCP, nhưng có thể tùy chỉnh để mở rộng dải IP.

Để thêm bớt VMnet ta có thể chọn **Add Network** và **Remove Network**. Khi bạn tạo VMnet mới, thì trên máy thật sẽ tạo ra những card mạng ảo tương ứng với VMnet đó, dùng để kết nối Virtual Switch với máy thật, giúp chúng liên lạc với nhau. Riêng VMnet0 kết nối trực tiếp với card mạng vật lý (bridged) nên không tạo VMnet.



```
C:\WINDOWS\system32\cmd. x + v
Connection-specific DNS Suffix . :
Ethernet adapter VMware Network Adapter VMnet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::37ba:2343:8f00:c050%18
IPv4 Address. . . . . : 10.10.19.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::9270:6b5e:3dbd:3ecc%33
IPv4 Address. . . . . : 192.168.158.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

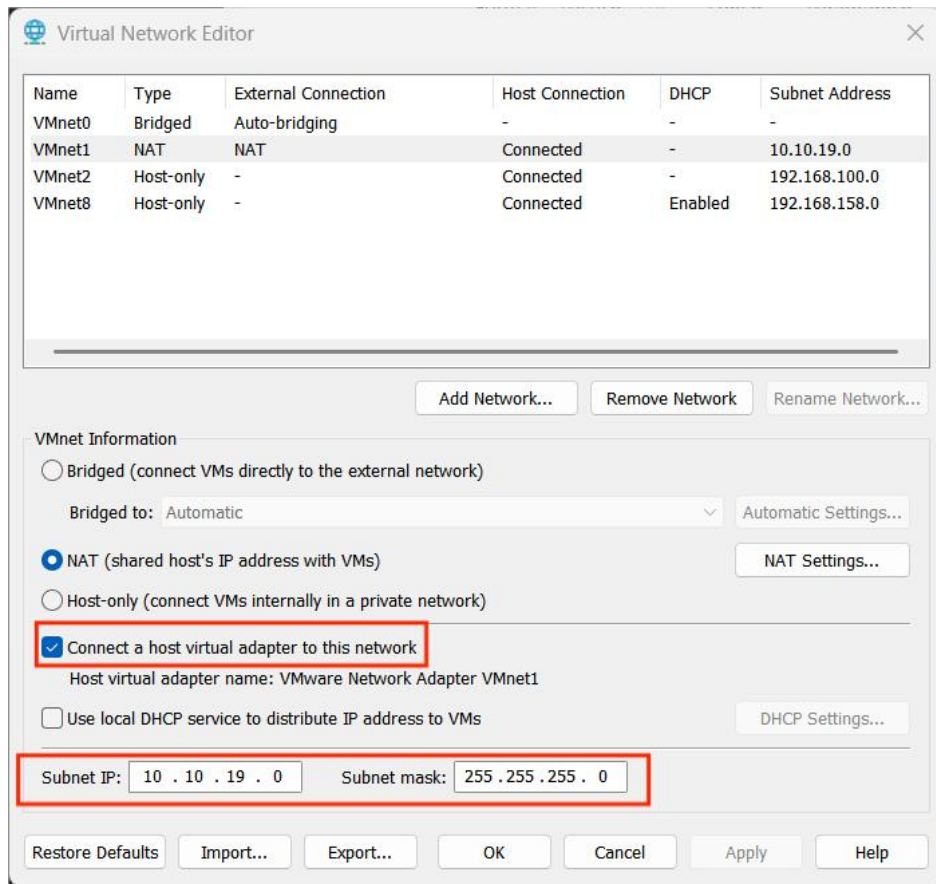
Ethernet adapter VMware Network Adapter VMnet2:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::87b4:5ddc:22c:365f%34
IPv4 Address. . . . . : 192.168.100.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

Hình 2. Card mạng tương ứng trên máy thật

Có thể thay đổi dải IP VMnet bằng cách nhấn vào VMnet muốn đổi địa chỉ, điền dải IP mong muốn vào ô Subnet IP và điền Subnet mask.

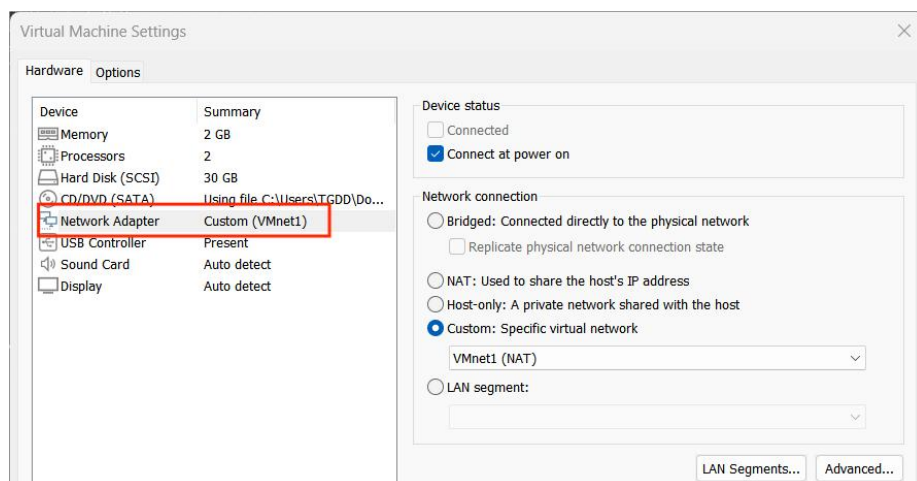
Để card mạng ảo kết nối máy thật với các VMnet, bạn cần tích ô **Connect a host virtual adapter to ...**



Hình 3. Card mạng ảo kết nối máy thật

## 2.2. Card mạng ảo (Virtual Network Adapter)

Khi tạo một máy ảo mới, card mạng được tạo ra cho máy ảo. Nó là phần cứng ảo trong mỗi máy ảo, kết nối máy ảo với một switch ảo.



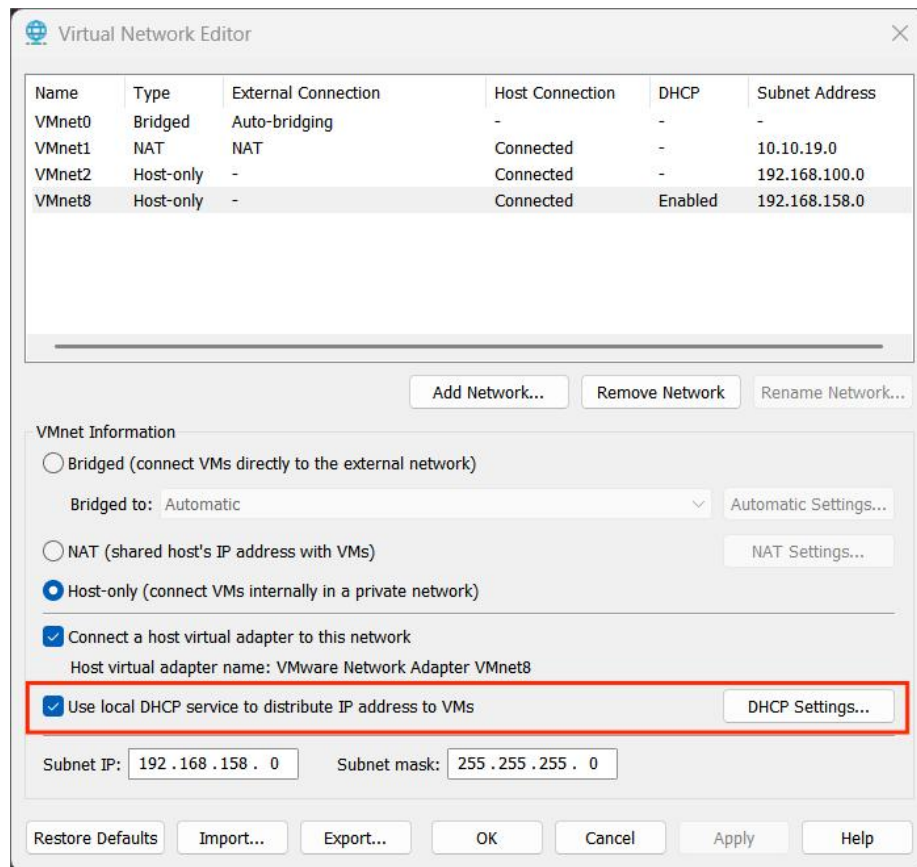
Hình 4. Virtual Network Adapter

## 2.3. DHCP Server ảo (Virtual DHCP Server)

DHCP (Dynamic Host Configuration) server ảo đảm nhiệm việc cung cấp địa chỉ IP cho các máy ảo trong việc kết nối máy ảo vào các Switch ảo không có tính năng

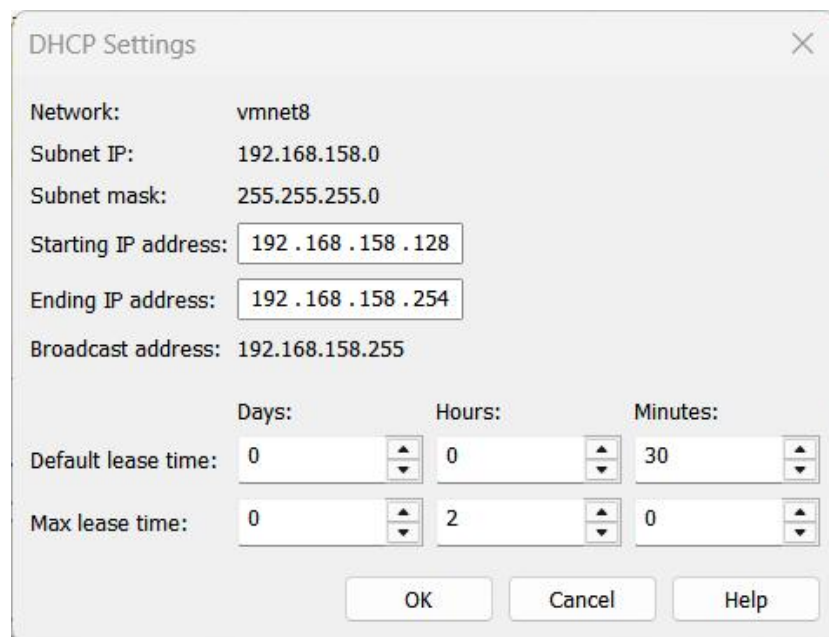


Bridged. DHCP server ảo cấp phát địa chỉ IP cho các máy ảo có kết nối với VMnet Host-only và NAT.



Hình 5. Virtual DHCP Service

Nếu muốn sử dụng chức năng này, cần tích vào ô **User local DHCP service...** .  
**Nếu muốn tùy chỉnh DHCP, chọn DHCP Settings:**



Hình 6. DHCP Settings

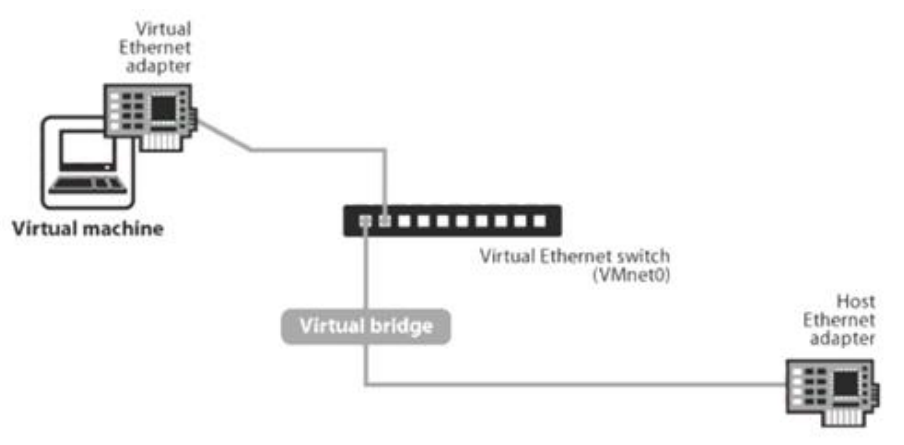
## 2.4. Thiết bị NAT

Trong cấu hình NAT, thiết bị NAT truyền dữ liệu mạng giữa một hoặc nhiều máy ảo với mạng bên ngoài, xác định các gói dữ liệu đến từ mỗi máy ảo và gửi chúng đến máy đích.

## 2.5. Cấu hình kết nối mạng

VMware có thể cấu hình kết nối mạng dạng bridged, NAT, Host-only cho các máy ảo. Khi cài Workstation Pro 17, có 3 switch được cài mặc định: VMnet0 (Bridged), VMnet1 (Host-only), VMnet8 (NAT).

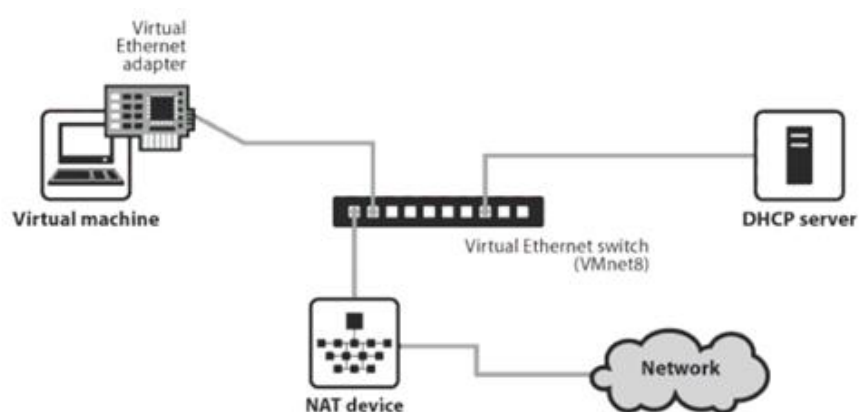
### a. Bridged



Hình 7. Bridged mode

- Máy ảo kết nối trực tiếp với mạng vật lý, giống như một máy thật, dễ dàng kết nối Internet.
- Có thể nhận địa chỉ IP từ router/DHCP thật.
- Dùng để giả lập một hệ thống mạng thực tế.
- Nhược điểm: Dễ dàng mất mạng do phụ thuộc vào card mạng thật

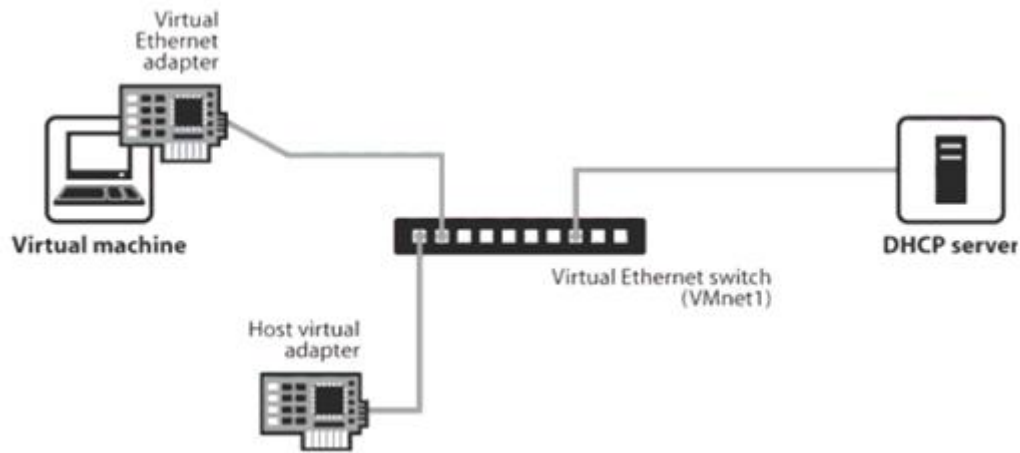
### b. NAT



Hình 8. NAT mode

- Máy ảo kết nối internet thông qua máy host, máy host đóng vai trò là gateway, giúp máy ảo truy cập internet.
- Trong cấu hình này, máy ảo nhận địa chỉ IP của mạng ảo từ DHCP server ảo.

### c. Host-Only



Hình 9. Host-only mode

- Máy ảo chỉ có thể giao tiếp với máy host và các máy ảo khác trong cùng mạng ảo, tách biệt hoàn toàn với mạng vật lý.
- Không có kết nối ra internet (trừ khi thêm cổng NAT hoặc bridge).
- Dùng để mô phỏng mạng nội bộ riêng.

# I. NỘI DUNG THỰC HÀNH

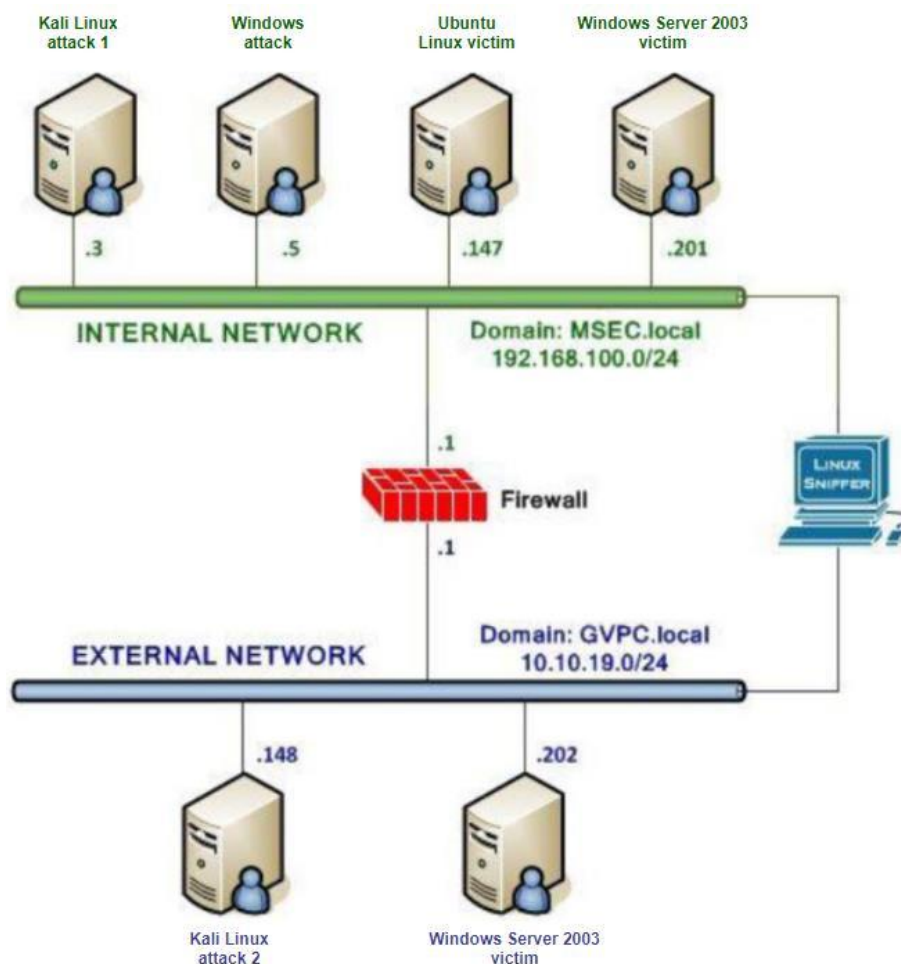
## 1. Chuẩn bị môi trường

- Phần mềm VMWare Workstation
- Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows và Linux.
- File cài đặt tường lửa Pfsense

## 2. Thực hành

### 2.1. Cấu hình topo mạng

Topo mạng như mô tả dưới đây:



Hình 10. Topo mạng cần chuẩn bị

#### a. Cấu hình hệ thống

- Cấu hình các máy Internal Network:
  - Máy Kali Linux Attack 1:

```

(nguyenvanhungb22dcat136@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:febc:1b61 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:bc:1b:61 txqueuelen 1000 (Ethernet)
    RX packets 1 bytes 60 (60.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2878 (2.8 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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Hình 11. Máy Kali Linux attack 1

- Máy Windows attack:

The image shows two overlapping windows from a Windows system. The background window is a command prompt titled 'C:\Windows\system32\cmd.exe' showing the output of the 'ipconfig' command. The foreground window is titled 'C:\WINDOWS\system32\CMD' and shows the output of the 'date' and 'echo' commands.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\NguyenVanHungAT136>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7f95:7615:3ece:3610%4
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\Users\NguyenVanHungAT136>

C:\WINDOWS\system32\CMD
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>echo %date% %time% Nguyen Van Hung B22DCAT136
Sat 03/15/2025 15:47:30.92 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

```

Hình 12. Máy Windows attack

- Ubuntu Linux victim:

The image shows two overlapping windows. The background window is an Ubuntu terminal titled 'ubuntu@NguyenVanHungB22DCAT136: ~' showing the output of the 'ip a' command. The foreground window is a Windows command prompt titled 'C:\WINDOWS\system32\cmd.exe' showing the output of the 'date' and 'echo' commands.

```

ubuntu@NguyenVanHungB22DCAT136: ~
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN
    link/ether 00:0c:29:ce:a1:84 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fece:a184/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@NguyenVanHungB22DCAT136: ~
$

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.27813.1000]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TGDD>date
The current date is: Sat 03/15/2025
Enter the new date: (mm-dd-yy)

C:\Users\TGDD>echo Nguyen Van Hung B22DCAT136
Nguyen Van Hung B22DCAT136

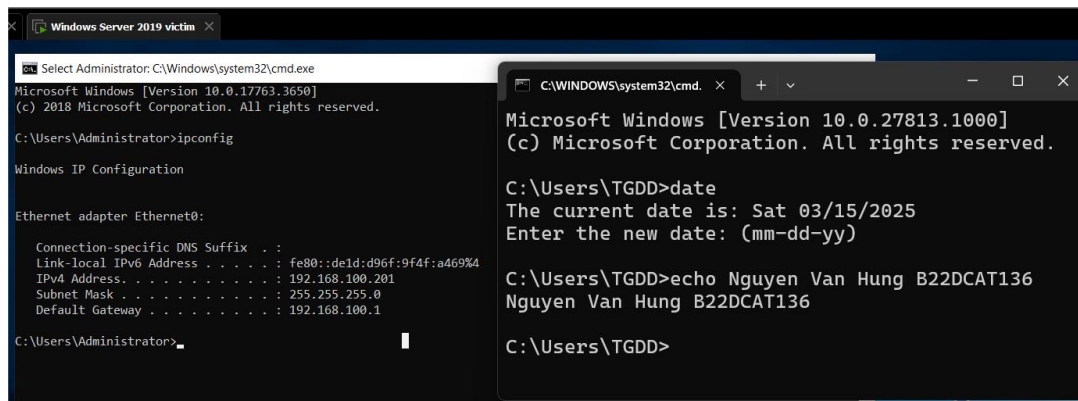
C:\Users\TGDD>

```

Hình 13. Ubuntu Linux victim

- Windows Server 2019 victim:

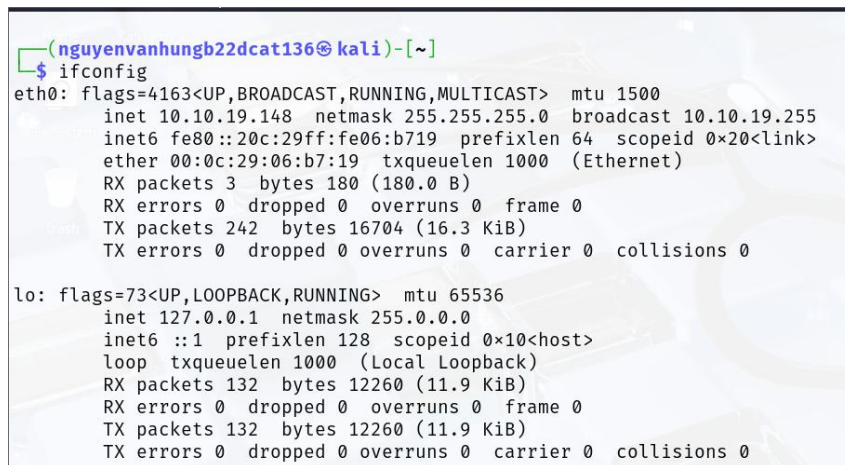




Hình 14. Windows Server victim

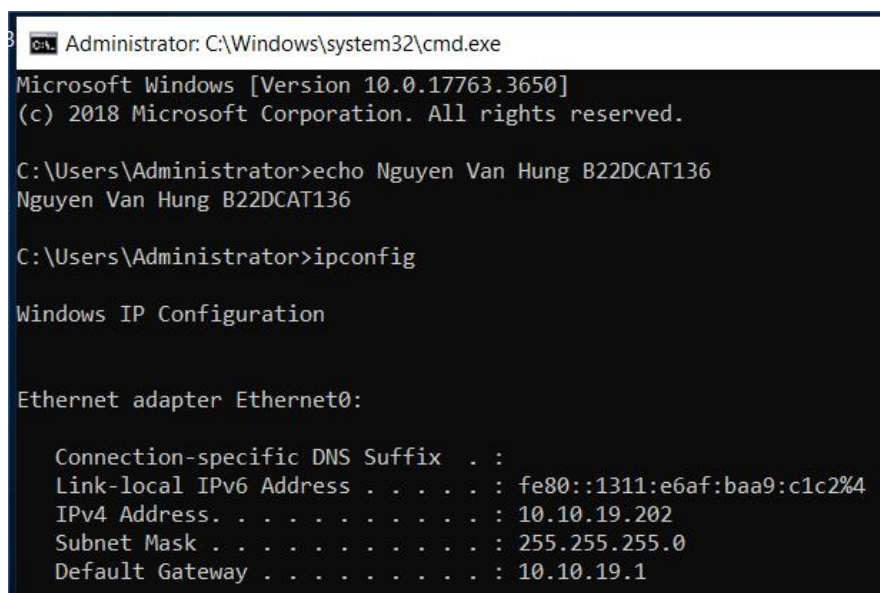
- Cấu hình các máy External Network:

■ Máy Kali Linux Attack 2:



Hình 15. Máy Kali Linux attack 2

■ Máy Windows Server 2019 victim:



Hình 16. Máy Windows Server 2019 victim

Cấu hình tường lửa:

```
C:\WINDOWS\system32\cmd. x + v - □

C:\Users\TGDD>echo %date% Nguyen Van Hung B22DCAT136
Wed 03/19/2025 Nguyen Van Hung B22DCAT136

C:\Users\TGDD>

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.10.19.1/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
```

Hình 17. Cấu hình pfSense

### b. Ping các máy với nhau

Ping từ máy Kali Linux Attack 1 (Internal) và pfSense LAN:

```
(nguyenvanhungb22dcat136@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc
link/loopback 00:00:00:00:00:00 brd 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
link/ether 00:0c:29:bc:1b:61 brd ff:ff:ff:
inet 192.168.100.3/24 brd 192.168.100.255
    valid_lft forever preferred_lft forever
inet6 fe80::20c:29ff:febc:1b61/64 scope li
    valid_lft forever preferred_lft forever

(nguyenvanhungb22dcat136@kali)-[~]
$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=1.69 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=2.35 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.754/1.597/2.353/0.655 ms

WAN (wan)      -> em0      -> v4: 10.10.19.1/24
LAN (lan)      -> em1      -> v4: 192.168.100.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.home.arpal/root]: ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3): 56 data bytes
64 bytes from 192.168.100.3: icmp_seq=0 ttl=64 time=1.054 ms
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=1.557 ms
^C
--- 192.168.100.3 ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.054/1.305/1.557/0.251 ms
[2.7.2-RELEASE][root@pfSense.home.arpal/root]:
```

Hình 18. Kết nối Kali Linux Attack (Internal) và pfSense LAN

Ping từ máy Window attack đến máy Kali Linux Attack 1 (Internal):

```

C:\Users\NguyenVanHungAT136>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::7f95:7615:3ece:3610%7
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1

C:\Users\NguyenVanHungAT136>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

Ping statistics for 192.168.100.3:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C

```

Hình 19. Kết nối từ Windows attack đến Kali Linux Attack 1 (Internal)

Ping từ máy Windows Server 2019 Victim (External) và pfSense WAN:

<pre> Administrator: C:\Windows\system32\cmd.exe Microsoft Windows [Version 10.0.17763.3650] (c) 2018 Microsoft Corporation. All rights reserved.  C:\Users\Administrator&gt;echo Nguyen Van Hung B22DCAT136 Nguyen Van Hung B22DCAT136  C:\Users\Administrator&gt;ipconfig  Windows IP Configuration  Ethernet adapter Ethernet0:      Connection-specific DNS Suffix  . :      Link-local IPv6 Address . . . . . : fe80::1311:e6af:baa9:c1c2%5     IPv4 Address. . . . . : 10.10.19.202     Subnet Mask . . . . . : 255.255.255.0     Default Gateway . . . . . : 10.10.19.1  C:\Users\Administrator&gt;ping 10.10.19.1  Pinging 10.10.19.1 with 32 bytes of data: Reply from 10.10.19.1: bytes=32 time&lt;1ms TTL=64  Ping statistics for 10.10.19.1:     Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),     Approximate round trip times in milli-seconds:         Minimum = 0ms, Maximum = 0ms, Average = 0ms Control-C </pre>	<pre> Enter an option: 7  Enter a host name or IP address: 10.10.19.202  PING 10.10.19.202 (10.10.19.202): 56 data bytes 64 bytes from 10.10.19.202: icmp_seq=0 ttl=128 time=1.882 ms 64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=3.101 ms 64 bytes from 10.10.19.202: icmp_seq=2 ttl=128 time=2.747 ms  --- 10.10.19.202 ping statistics --- 3 packets transmitted, 3 packets received, 0.0% packet loss round-trip min/avg/max/stddev = 1.882/2.576/3.101/0.512 ms </pre>
---	---

Hình 20. Kết nối Windows Server Victim (External) và pfSense WAN



Ping từ máy Windows Server 2019 Victim đến máy Kali Linux Attack 2 (External):

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>echo Nguyen Van Hung B22DCAT136
Nguyen Van Hung B22DCAT136

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1311:e6af:baa9:c1c2%4
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.10.19.1

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

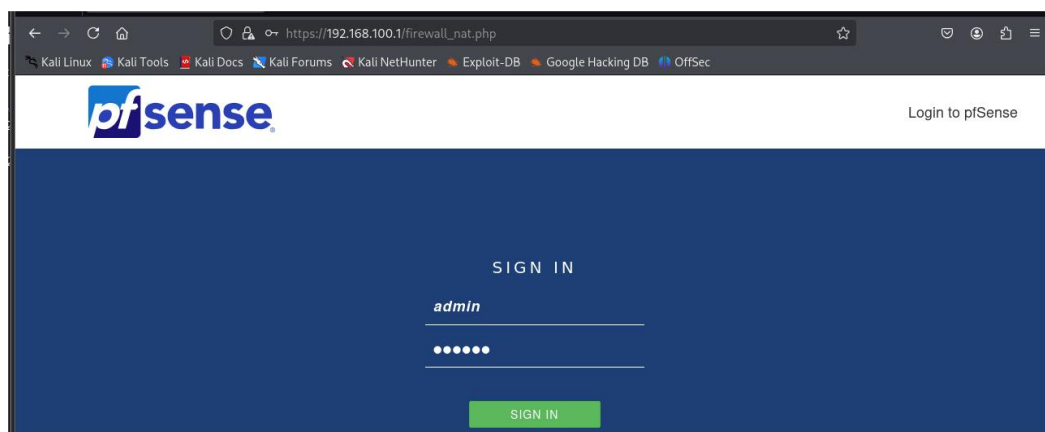
Ping statistics for 10.10.19.148:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hình 21. Kết nối Windows Server Victim và Kali Linux Attack 2 (External)

## 2.2. Cài đặt cấu hình pfSense firewall cho lưu lượng ICMP

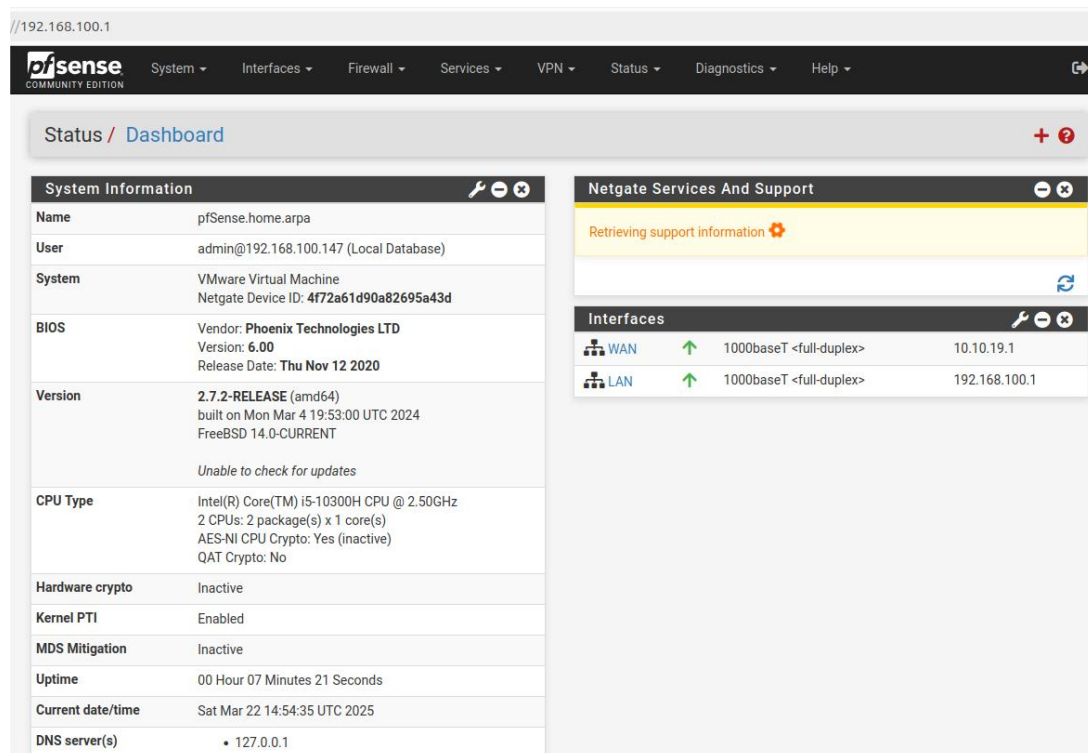
### a. Truy cập giao diện quản lý pfSense

Trên máy Linux Victim (Internal), truy cập **http://192.168.100.1** để vào giao diện web pfSense, thực hiện đăng nhập bằng tài khoản:



Hình 22. Đăng nhập pfSense

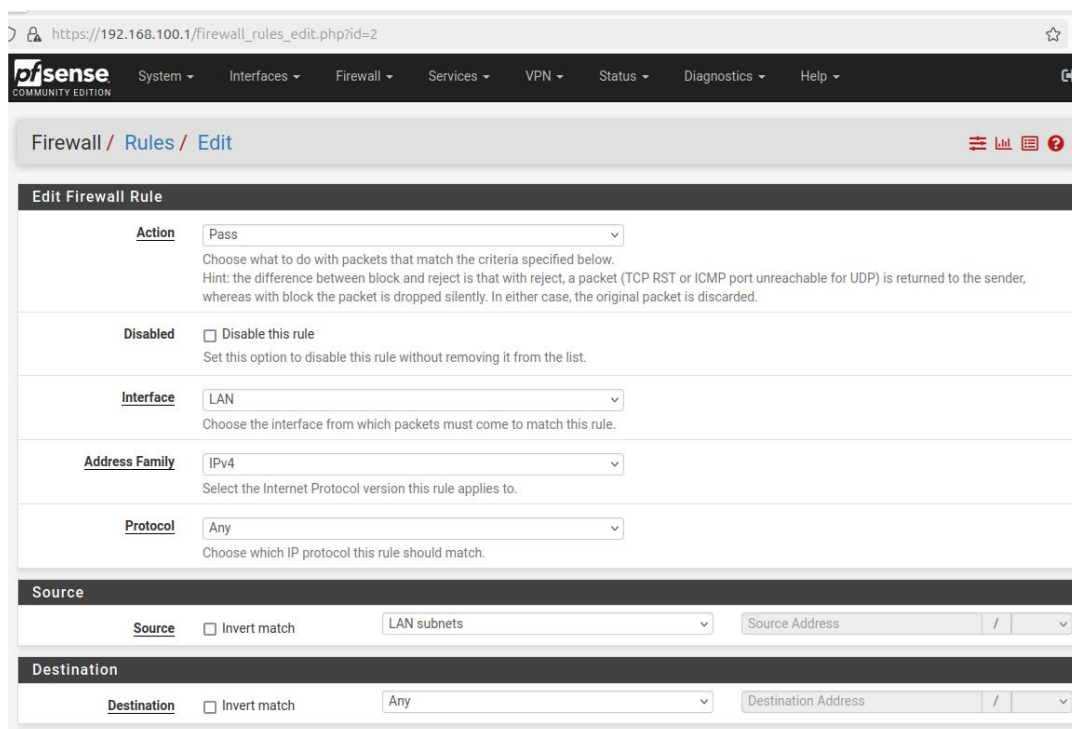
## Giao diện pfSense:



Hình 23. Giao diện pfSense

### b. Cấu hình cho phép ICMP từ Internal ra External

Chọn **Firewall** → **Rules** → **LAN**: Nhấn **Add** để thêm rule firewall cho mạng Internal.

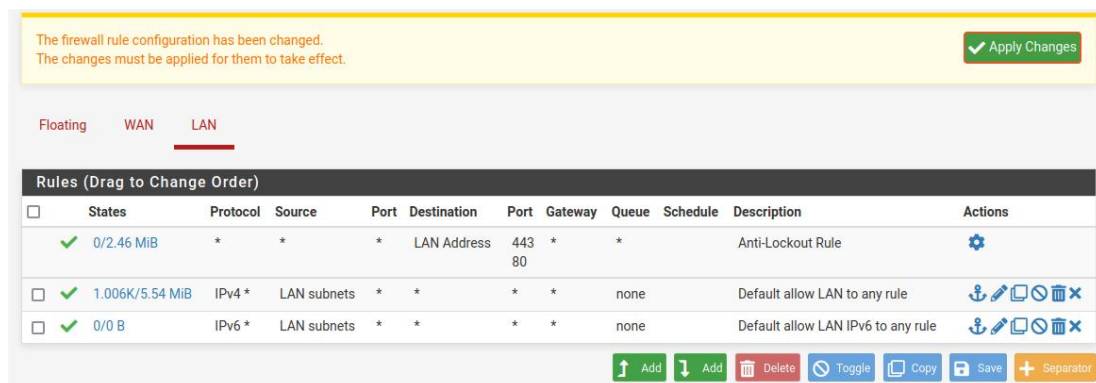


Hình 24. Cấu hình cho phép ICMP từ Internal ra External

Cấu hình rule:

- **Action: Pass** → Cho phép gói tin được đi qua
- **Interface: LAN** → Rule áp dụng cho lưu lượng từ mạng LAN
- **Protocol: Any hoặc ICMP** → Nếu chọn ICMP: chỉ cho phép gói tin ICMP (dùng cho ping, traceroute,...). Nếu chọn Any: mọi loại lưu lượng đều được phép đi ra.
- **Source: LAN subnets** → Chỉ các thiết bị trong mạng LAN (Internal network) mới có thể sử dụng rule này.
- **Destination: Any** → Cho phép gói tin gửi đến bất kỳ đâu trên Internet hoặc các mạng khác.

Nhấn **Save** → **Apply Changes** để lưu thay đổi.



Hình 25. Lưu thay đổi LAN

### c. Chặn ICMP từ External vào Internal

Chọn **Firewall** → **Rules** → **WAN**: Nhấn **Add** để thêm rule firewall cho mạng External.

Cấu hình rule:

- **Action: Block** → Chặn gói tin đi qua
- **Interface: WAN** → Rule này áp dụng cho lưu lượng từ mạng WAN
- **Protocol: ICMP** → Chặn gói tin ICMP
- **Source: Any** → Chặn tất cả các thiết bị từ bên ngoài.
- **Destination: LAN subnets** → Chặn ICMP khi nó đi đến mạng LAN

Nhấn **Save** → **Apply Changes** để lưu thay đổi.

**Edit Firewall Rule**

**Action** Block  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** ICMP  
Choose which IP protocol this rule should match.

**ICMP Subtypes** any  
Alternate Host  
Datagram conversion error  
Echo reply  
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**

**Source** ☐ Invert match Any Source Address /

**Destination**

**Destination** ☐ Invert match LAN subnets Destination Address /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule

Hình 26. Chặn ICMP từ External vào Internal

#### d. Cấu hình cho phép ICMP từ External đến pfSense WAN

Chọn **Firewall** → **Rules** → **WAN**: Nhấn **Add** để thêm rule firewall cho mạng External.

**Edit Firewall Rule**

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** WAN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** ICMP  
Choose which IP protocol this rule should match.

**ICMP Subtypes** any  
Alternate Host  
Datagram conversion error  
Echo reply  
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

**Source**

**Source** ☐ Invert match Any Source Address /

**Destination**

**Destination** ☐ Invert match WAN address Destination Address /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule

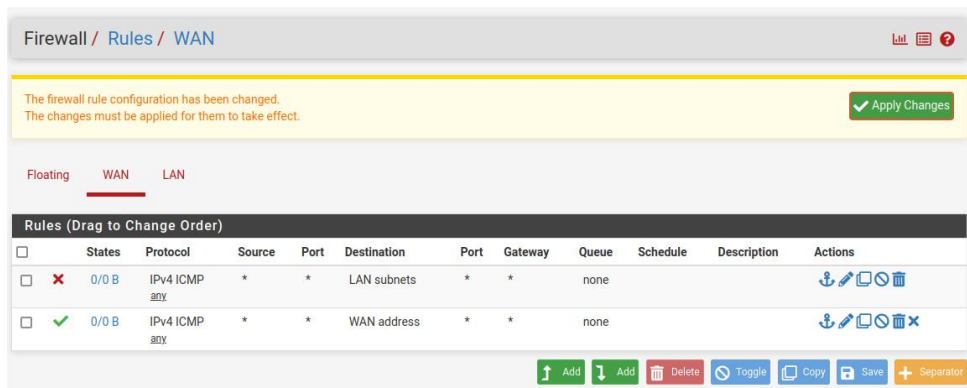
Hình 27. Chặn ICMP từ External vào Internal

Cấu hình rule:

- **Action: Pass**

- **Interface: WAN**
- **Protocol: ICMP**
- **Source: Any**
- **Destination: WAN address** → Chỉ cho phép ICMP đến địa chỉ WAN của pfSense, không vào mạng LAN.

Nhấn **Save** → **Apply Changes** để lưu thay đổi.



Hình 28. Lưu thay đổi WAN

### e. Kiểm tra kết quả

Từ máy Ubuntu Linux victim (Internal):

- Ping đến máy Kali Linux attack 2 (External): *ping 10.10.19.148*
- Ping đến pfSense WAN: *ping 10.10.19.1*

→ Thành công ping đến các máy ở mạng External

```
ubuntu@NguyenVanHungB22DCAT136:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:ce:a1:84 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fece:a184/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@NguyenVanHungB22DCAT136:~$ ping 10.10.19.148
PING 10.10.19.148 (10.10.19.148) 56(84) bytes of data.
64 bytes from 10.10.19.148: icmp_seq=1 ttl=63 time=1.73 ms
64 bytes from 10.10.19.148: icmp_seq=2 ttl=63 time=4.34 ms
^C
--- 10.10.19.148 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.728/3.032/4.336/1.304 ms
ubuntu@NguyenVanHungB22DCAT136:~$ 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=1.02 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.606 ms
^C
--- 10.10.19.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.606/0.814/1.022/0.208 ms
ubuntu@NguyenVanHungB22DCAT136:~$ ifconfig
```

Hình 29. Kiểm tra ping từ Internal ra ngoài

Từ máy Linux Attack (External):



- Ping đến máy Ubuntu Linux victim (Internal): *ping 192.168.100.147*
  - Ping đến pfSense (LAN): *ping 192.168.100.1*
- Thành công cấu hình không cho phép ping vào trong mạng Internal

```

nguyenvanhungb22dcat136@kali: ~
File Actions Edit View Help
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:0c:29:06:b7:19 brd ff:ff:ff:ff:ff:ff
   inet 10.10.19.148/24 brd 10.10.19.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::20c:29ff:fe06:b719/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

nguyenvanhungb22dcat136@kali:~$
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data.
^C
— 192.168.100.147 ping statistics —
2 packets transmitted, 0 received, 100% packet loss, time 1024ms

nguyenvanhungb22dcat136@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=0.785 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.791 ms
^C
— 10.10.19.1 ping statistics —
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.785/0.788/0.791/0.003 ms

nguyenvanhungb22dcat136@kali:~$
$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
^C
— 192.168.100.1 ping statistics —
7 packets transmitted, 0 received, 100% packet loss, time 6142ms

```

Hình 30. Kiểm tra chặn ping từ External vào Internal

Để kiểm tra có bao nhiêu cổng TCP mở trên giao diện mạng trong và ngoài của pfSense, mở một máy thuộc mạng Internal, quét cổng bằng nmap:

```

nguyenvanhungb22dcat136@kali:~$
$ nmap -p- 192.168.100.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 12:14 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00070s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 00:50:56:C0:00:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 117.57 seconds

nguyenvanhungb22dcat136@kali:~$
$ nmap -p- 10.10.19.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 12:17 EDT
Nmap scan report for 10.10.19.1
Host is up (0.00079s latency).
Not shown: 65532 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 117.59 seconds

nguyenvanhungb22dcat136@kali:~$
$ 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:29:06:b7:19 brd ff:ff:ff:ff:ff:ff
   inet 192.168.100.3/24 brd 192.168.100.255 scope global eth0

```

Hình 31. Kiểm tra cổng TCP

- Kiểm tra các cổng TCP mở trên pfSense LAN: *nmap -p- 192.168.100.1*
- Kiểm tra các cổng TCP mở trên pfSense WAN: *nmap -p- 10.10.19.1*

Quét tất cả các cổng TCP (1- 65535): -p-

Kết quả:

- 53/tcp (domain) → Cổng của DNS server, có thể được sử dụng để phân giải tên miền.
- 80/tcp (http) → Cổng của HTTP web server, thường dùng để phục vụ trang web không mã hóa (không có HTTPS).
- 443/tcp (https) → Cổng của HTTPS web server, phục vụ các trang web có mã hóa SSL/TLS (bảo mật hơn HTTP).

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

### a. Cấu hình Port Forwarding (NAT)

Trên máy Kali Linux Victim (Internal), truy cập giao diện web của pfSense.

Vào **Firewall** → **NAT** → **Port Forward**, nhấn **Add** để tạo rule mới

Firewall / NAT / Port Forward / Edit

**Edit Redirect Entry**

☐ Disabled ☐ Disable this rule

**No RDR (NOT)** ☐ Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface** WAN  
Choose which interface this rule applies to. In most cases "WAN" is specified.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source**

**Destination** ☐ Invert match. WAN address Address/mask

**Destination port range** SSH From port Custom To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** Address or Alias 192.168.100.147  
Type Address  
Enter the internal IP address of the server on which to map the ports, e.g. 192.168.1.12 for IPv4.  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

**Redirect target port** SSH Port Custom  
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

**Description** Forward SSH traffic to Internal Ubuntu Linux Victim  
A description may be entered here for administrative reference (not parsed).

**No XMLRPC Sync** ☐ Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection** Use system default

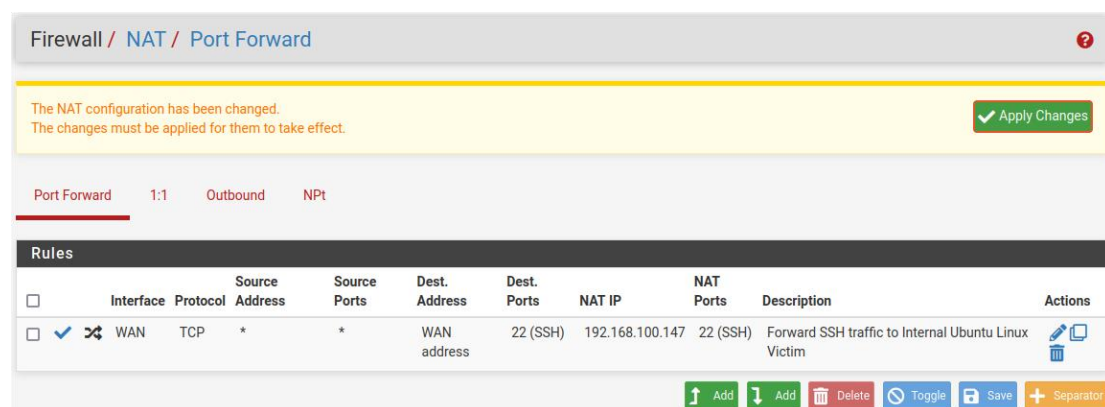
**Filter rule association**

Hình 32. Cấu hình Port Forwarding

Cấu hình Rule:

- Interface: WAN
- Protocol: TCP
- Destination: Chọn WAN Address
- Destination Port Range: SSH (22)
- Redirect Target IP: 192.168.100.147 (IP của máy Linux victim trong mạng Internal)
- Redirect Target Port: SSH (22)

Nhấn **Save** và sau đó nhấn **Apply Changes**.



Hình 33. Apply Changes Port Forward

### b. Kiểm tra truy cập ssh

Mở máy bên ngoài Kali Linux Attack 2 (External), thực hiện ssh đến địa chỉ IP của tường lửa pfSense (10.10.19.1): `ssh ubuntu@10.10.19.1`

Giải thích: ubuntu là username máy Linux victim trong mạng Internal.

```
(nguyenvanhungb22dcat136@kali)-[~]
$ 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:29:06:b7:19 brd ff:ff:ff:ff:ff:ff
   inet 10.10.19.148/24 brd 10.10.19.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::20c:29ff:fe06:b719/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever

(nguyenvanhungb22dcat136@kali)-[~]
$ ssh ubuntu@10.10.19.1
ubuntu@10.10.19.1's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x86_64)

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



Hình 34. SSH đến địa chỉ IP tường lửa pfSense

Kiểm tra IP máy: *ip a*

```
(nguyenvanhungb22dcat136@kali)-[~]
$ ssh ubuntu@10.10.19.1
ubuntu@10.10.19.1's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-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.

104 updates can be applied immediately.
48 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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Mar 23 03:17:30 2025 from 10.10.19.148
ubuntu@nguyenvanhungb22dcat136:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:ce:a1:84 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.100.147/24 brd 192.168.100.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fece:a184/64 scope link
        valid_lft forever preferred_lft forever
```

Hình 35. Kiểm tra IP

IP máy là 192.168.100.147 → Thành công chuyển hướng lưu lượng

### c. Kiểm tra cổng được phép truy cập

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*

```
(nguyenvanhungb22dcat136@kali)-[~]
$ nmap 192.168.100.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-22 16:29 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00098s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:02 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.11 seconds

(nguyenvanhungb22dcat136@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:febc:1b61 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:bc:1b:61 txqueuelen 1000 (Ethernet)
    RX packets 261 bytes 27692 (27.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2364 bytes 150404 (146.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Hình 36. Kiểm tra cổng

Kết quả: 3306/tcp → Cổng mặc định của MySQL database server, dùng để quản lý và truy vấn cơ sở dữ liệu.

## TÀI LIỆU THAM KHẢO

- [1] <https://www.engisv.info/?p=134>
- [2] <https://www.makeuseof.com/whats-the-difference-nat-bridge-host-only-network-modes/>
- [3] <https://github.com/ducnc/vmware-workstation-network>
- [4] <https://dummytip.com/giai-ngo-virtualization-phan-5-3-che-do-vmware-network-configuration-ma-ban-nhat-dinh-phai-biet/>