

**ĐẠI HỌC BÁCH KHOA HÀ NỘI**  
**TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG**

————— \* —————



**BÁO CÁO TUẦN 2**

Môn học: Project II (IT - 3931)

Đề tài: Network Security with IDS/IPS: Detection and Prevention of  
Network Attacks in a Virtualized Environment

**Sinh viên thực hiện:**

**Ngô Trung Hiếu - 20225316**

**Kỹ thuật máy tính 04 – K67**

**Giảng viên hướng dẫn:**

**Nguyễn Quốc Khánh**

**Hà Nội – 2025**

## Mục lục

I.	Mục tiêu.....	4
II.	Topology mạng.....	4
III.	Các bước thiết lập và mô phỏng .....	5
1.	Tạo và cấu hình mạng cho các máy ảo .....	5
2.	Cài đặt pfsense .....	7
3.	Cấu hình địa chỉ IP cho máy ảo attacker và victim .....	9
4.	Cấu hình port forwarding.....	12
5.	Kiểm tra kết nối giữa các máy ảo .....	17
IV.	Đánh giá và kết luận .....	19



## I. Mục tiêu

- Thiết lập topology 3 máy ảo (Attacker — pfSense — Victim).
- Cấu hình WAN/LAN trên pfSense, cấu hình routing và firewall rules.
- Thực hiện kiểm tra kết nối (ICMP/ping) và port forwarding để truy cập dịch vụ nội bộ.

## II. Topology mạng

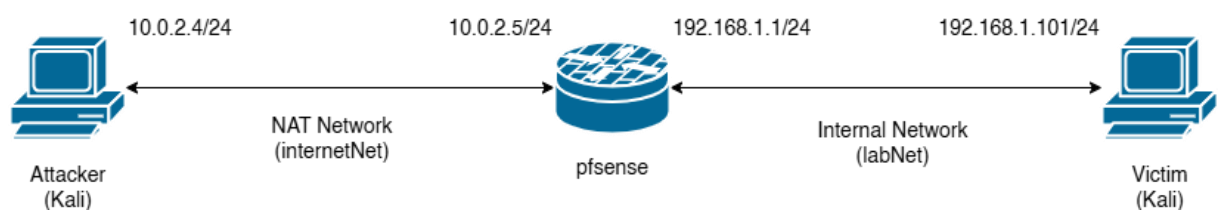


Figure 1: Topology mạng

Sơ đồ bao gồm hai mạng NAT Network (internetNet) và Internal Network (labNet), pfSense đứng giữa thực hiện NAT/Firewall và có thể truy cập Internet.

### Bảng cấu hình IP

VM	Adapter	Network name	IP	Gateway	OS
Attacker	Adapter 1	internetNet	10.0.2.4/24	10.0.2.5	Kali
pfSense	WAN (Adapter 1)	internetNet	10.0.2.5/24		FreeBSD
pfSense	LAN (Adapter 2)	labNet	192.168.1.1/24		FreeBSD
Victim	Adapter 1	labNet	192.168.1.101/24	192.168.1.1	Kali

### III. Các bước thiết lập và mô phỏng

#### 1. Tạo và cấu hình mạng cho các máy ảo

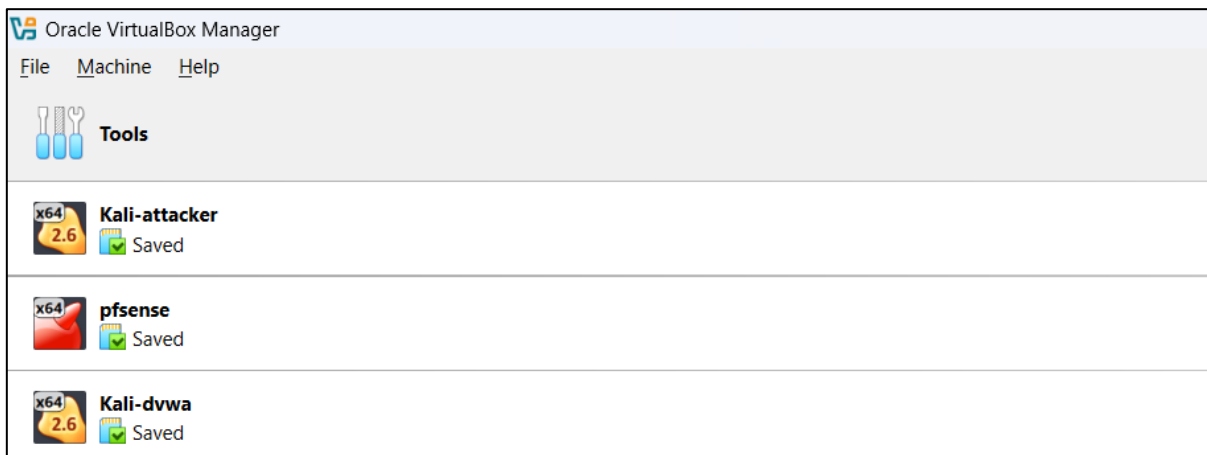


Figure 2: Tạo 3 máy ảo attacker, pfsense, và victim

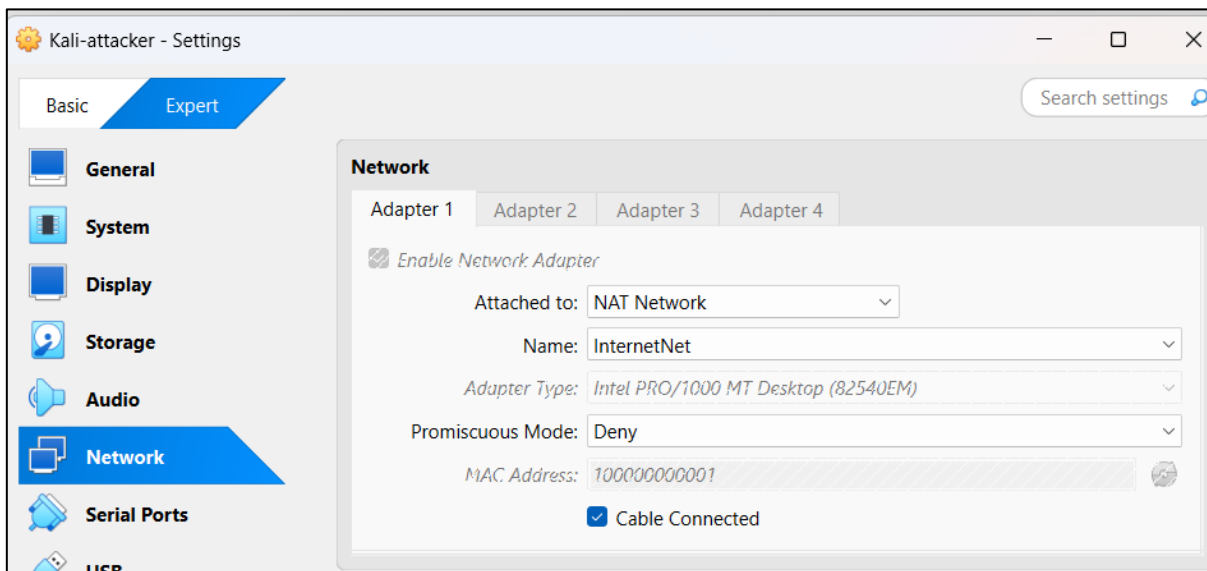


Figure 3: Cấu hình mạng cho attacker

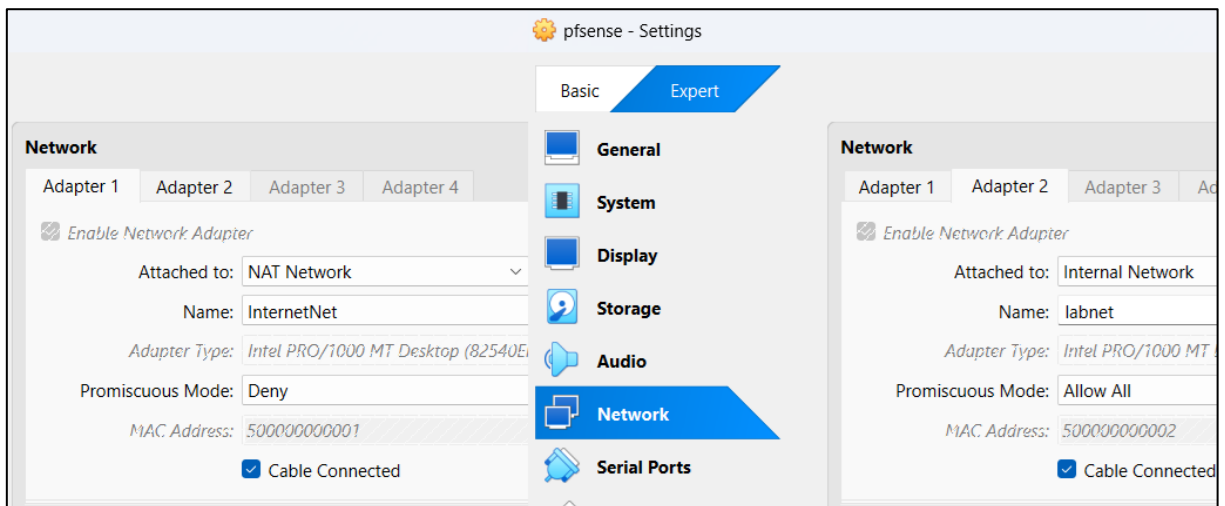


Figure 4: Cấu hình mạng cho pfSense

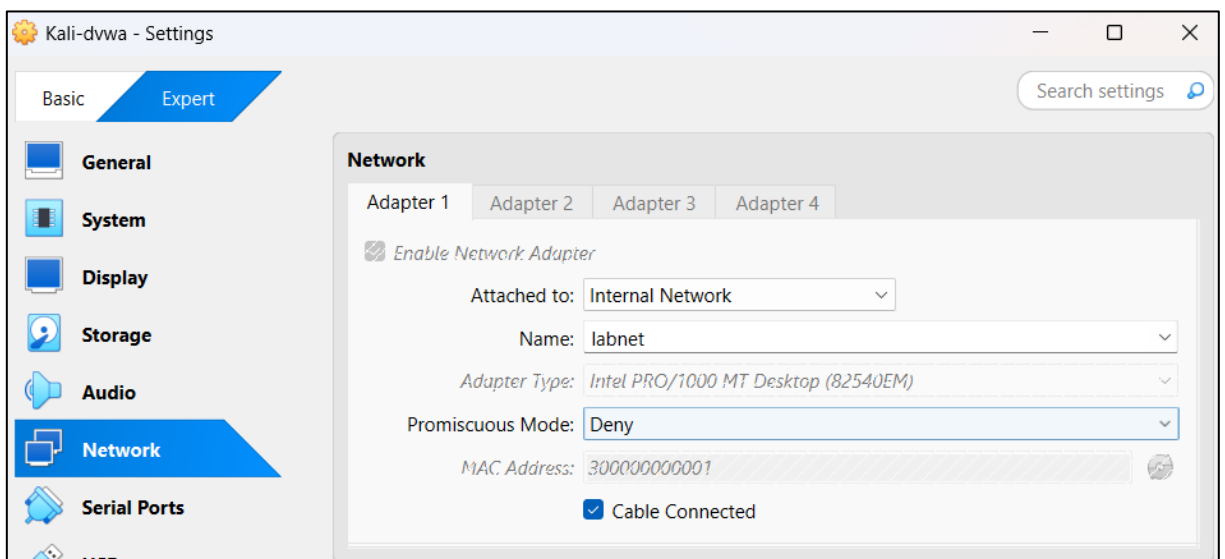


Figure 5: Cấu hình mạng cho victim

## 2. Cài đặt pfsense

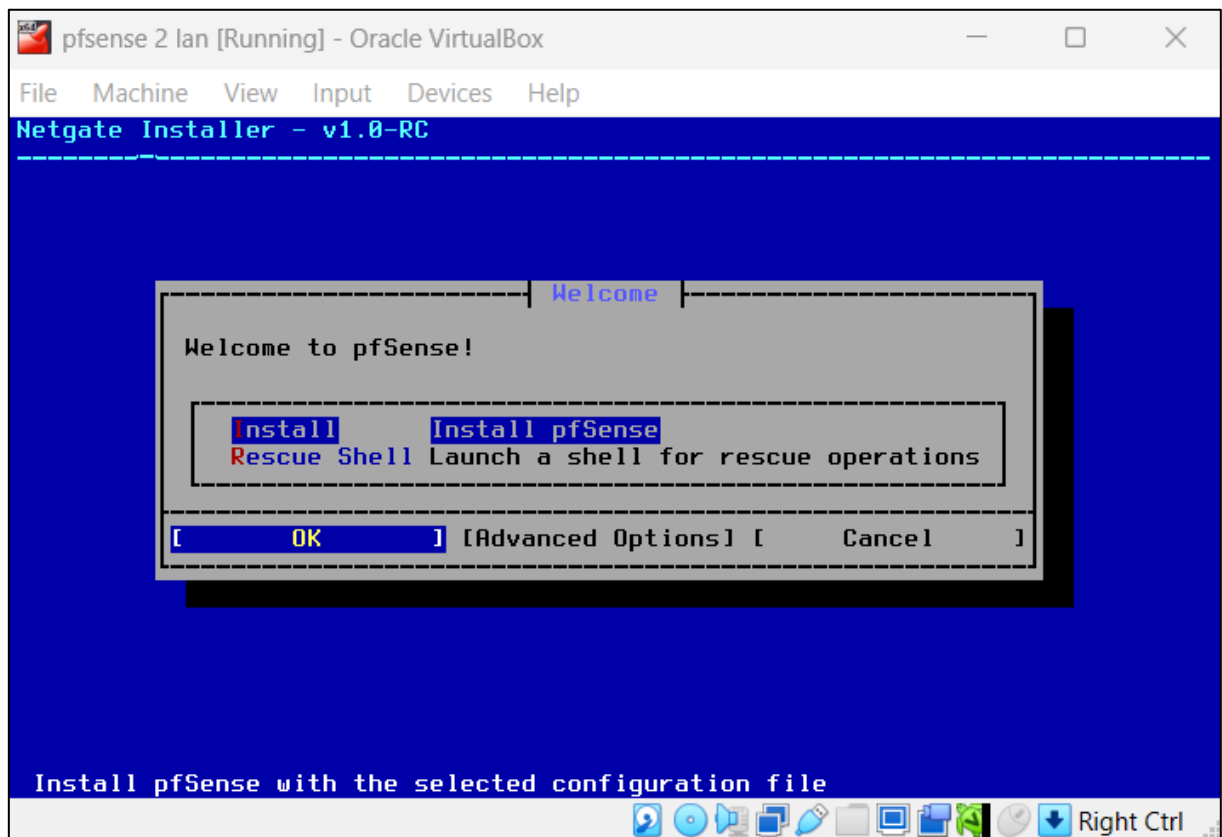


Figure 6: Cài đặt pfsense

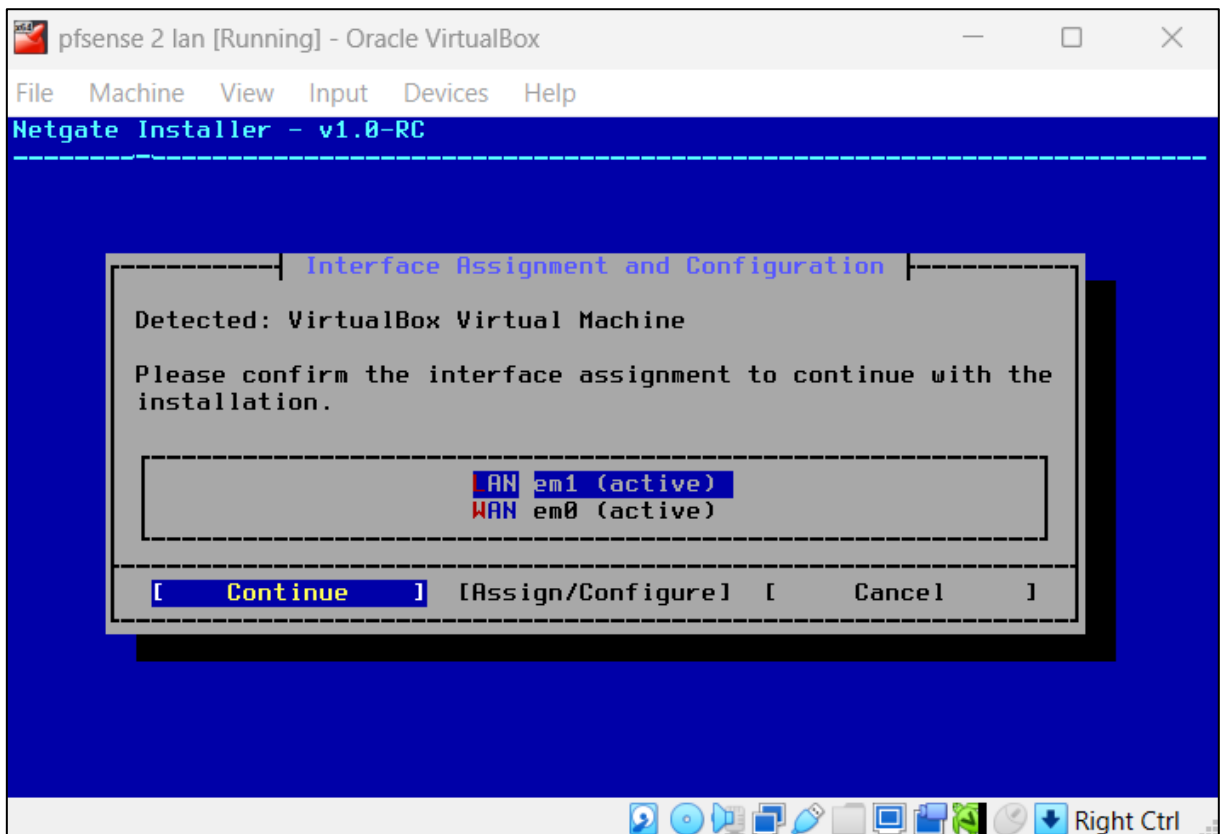


Figure 7: Gán interface với cấu hình mạng ở virtualbox

Sau khi cài đặt và reboot lại máy ảo, ta sẽ thấy màn hình chính của máy pfsense

```

8) Shell
Enter an option:

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: a6868047b9908627b94e
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.5/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address      11) Restart GUI
3) Reset admin account and password 12) PHP shell + pfSense tools
4) Reset to factory defaults        13) Update from console
5) Reboot system                    14) Enable Secure Shell (sshd)
6) Halt system                      15) Restore recent configuration
7) Ping host                        16) Restart PHP-FPM
8) Shell

Enter an option: 1

```

Figure 8: Màn hình chính của pfsense

Pfsense sẽ bao gồm 2 interface với địa chỉ IP lần lượt 10.0.2.5/24 và 192.168.1.1/24, tương ứng với 2 mạng WAN (NAT) và LAN.



### 3. Cấu hình địa chỉ IP cho máy ảo attacker và victim

Ta sẽ cấu hình DHCP để pfSense có thể tự động gán địa chỉ IP cho attacker và victim. Cấu hình 2 máy ảo này sẽ giống nhau nên ta sẽ làm với máy ảo attacker thôi, làm tương tự với máy ảo victim.

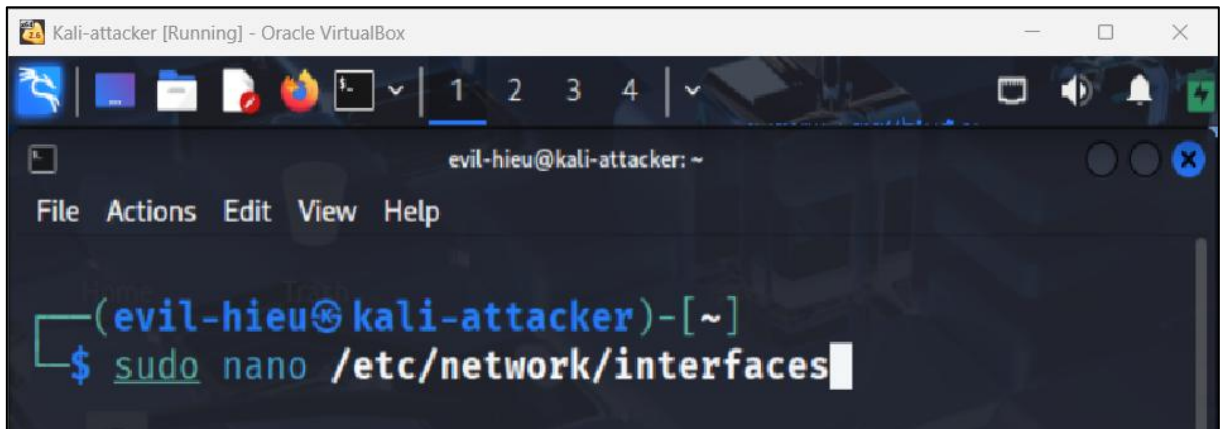


Figure 9: Vào file cấu hình mạng

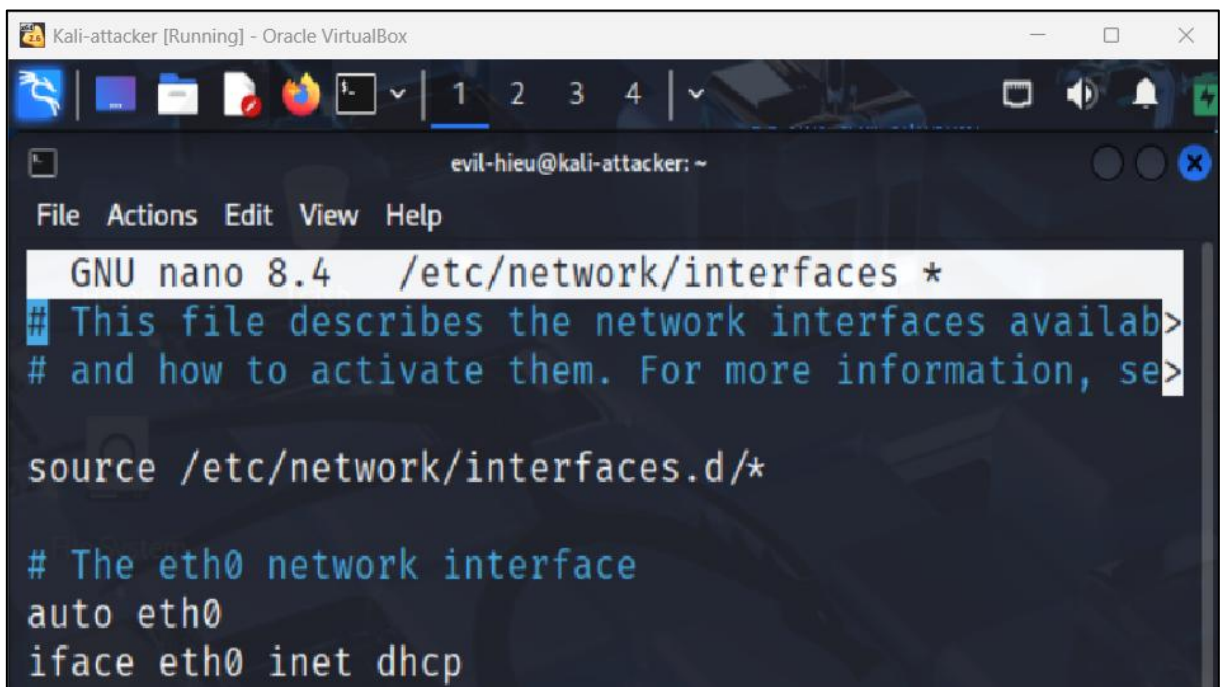
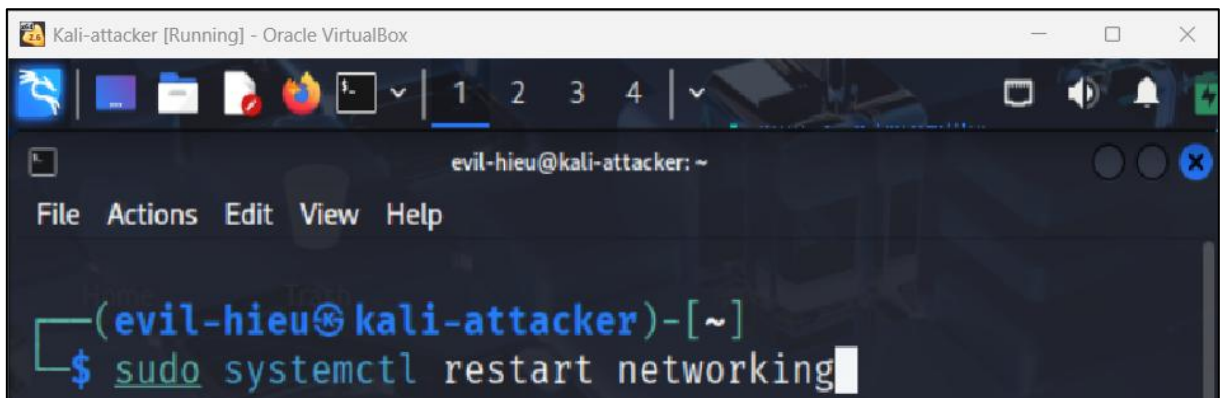


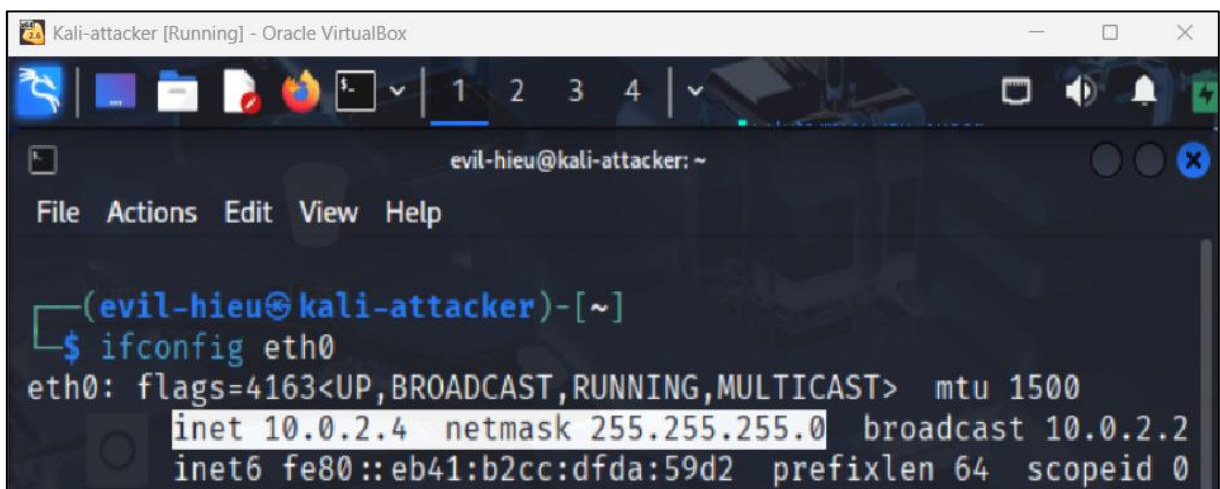
Figure 10: Thông tin cấu hình dhcp của interface eth0

Để áp dụng cấu hình mạng mới từ `/etc/network/interfaces` mà không cần khởi động lại máy. Lệnh **`sudo systemctl restart networking`** sẽ dừng/khởi động lại service quản lý interface, đưa cấu hình mới vào hoạt động (down/up các interface liên quan). Ngoài ra cần quyền sudo.



```
Kali-attacker [Running] - Oracle VirtualBox
evil-hieu@kali-attacker: ~
File Actions Edit View Help
(evil-hieu@kali-attacker)-[~]
$ sudo systemctl restart networking
```

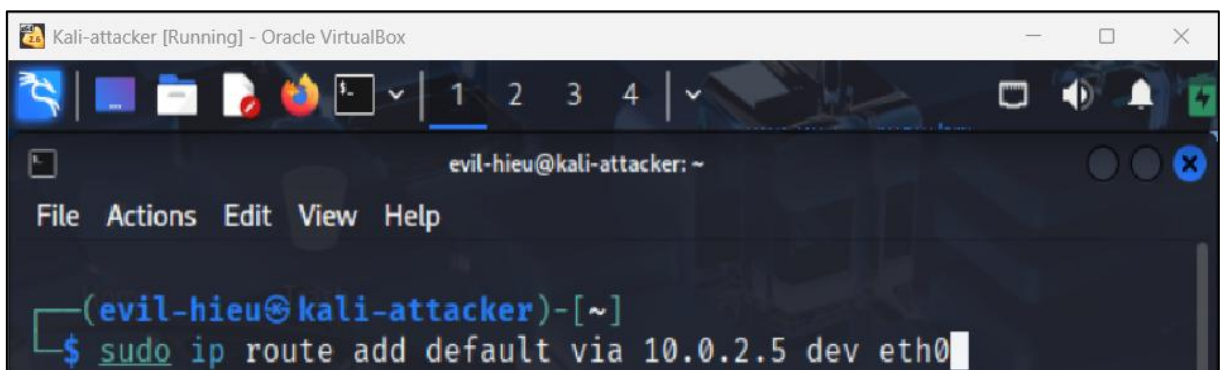
Figure 11: Lệnh khởi động lại service quản lý interface



```
Kali-attacker [Running] - Oracle VirtualBox
evil-hieu@kali-attacker: ~
File Actions Edit View Help
(evil-hieu@kali-attacker)-[~]
$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.2
    inet6 fe80::eb41:b2cc:dfda:59d2 prefixlen 64 scopeid 0
```

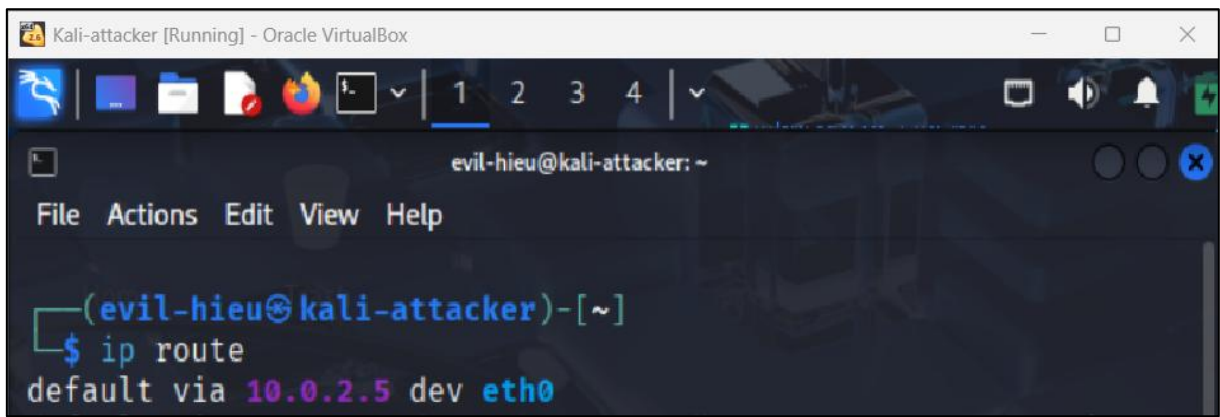
Figure 12: Địa chỉ IP của interface eth0 trên máy attacker

Sau đó ta cần gán default gateway cho máy attacker, để khi kiểm tra kết nối bằng lệnh ping đến victim ta sẽ gửi gói tin đến pfsense.



```
Kali-attacker [Running] - Oracle VirtualBox
evil-hieu@kali-attacker: ~
File Actions Edit View Help
(evil-hieu@kali-attacker)-[~]
$ sudo ip route add default via 10.0.2.5 dev eth0
```

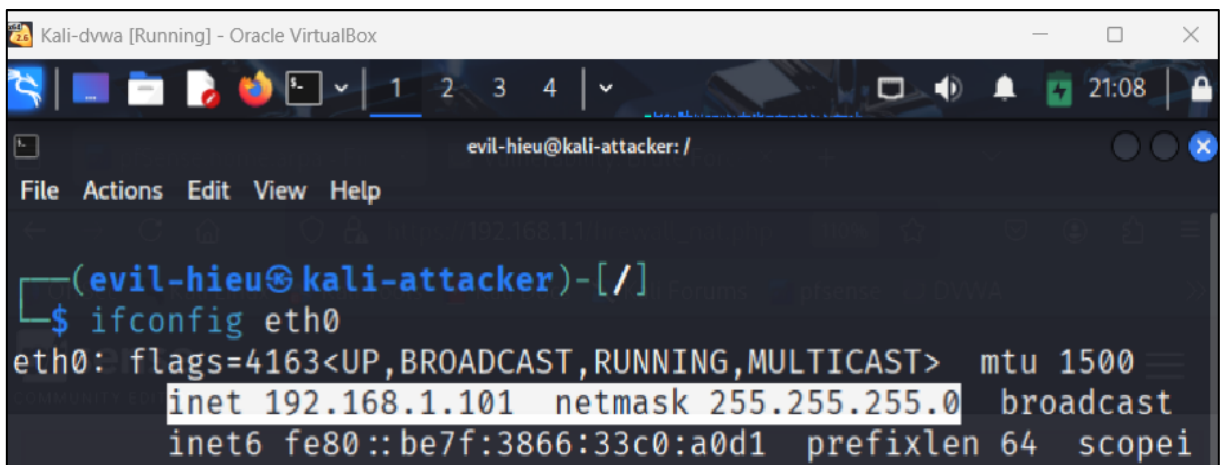
Figure 13: Gán default gateway



```
evil-hieu@kali-attacker: ~  
File Actions Edit View Help  
(evil-hieu@kali-attacker)-[~]  
$ ip route  
default via 10.0.2.5 dev eth0
```

Figure 14: Kiểm tra kết quả sau khi gán default gateway

Với các cài đặt trên, thì máy ảo victim có thể làm tương tự.



```
evil-hieu@kali-attacker: /  
File Actions Edit View Help  
(evil-hieu@kali-attacker)-[/]  
$ ifconfig eth0  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.101 netmask 255.255.255.0 broadcast  
    inet6 fe80::be7f:3866:33c0:a0d1 prefixlen 64 scopei
```

Figure 15: Địa chỉ IP của interface eth0 trên máy victim

Tuy nhiên, hiện tại thì máy ảo attacker chưa thể ping được dù về cơ bản 3 máy đã liên kết với nhau thông qua pfsense. Lý do là pfsense ở chế độ mặc định sẽ chặn các gói tin từ mạng bên ngoài vào mạng nội bộ (port forwarding), vậy nên ta phải cấu hình lại.

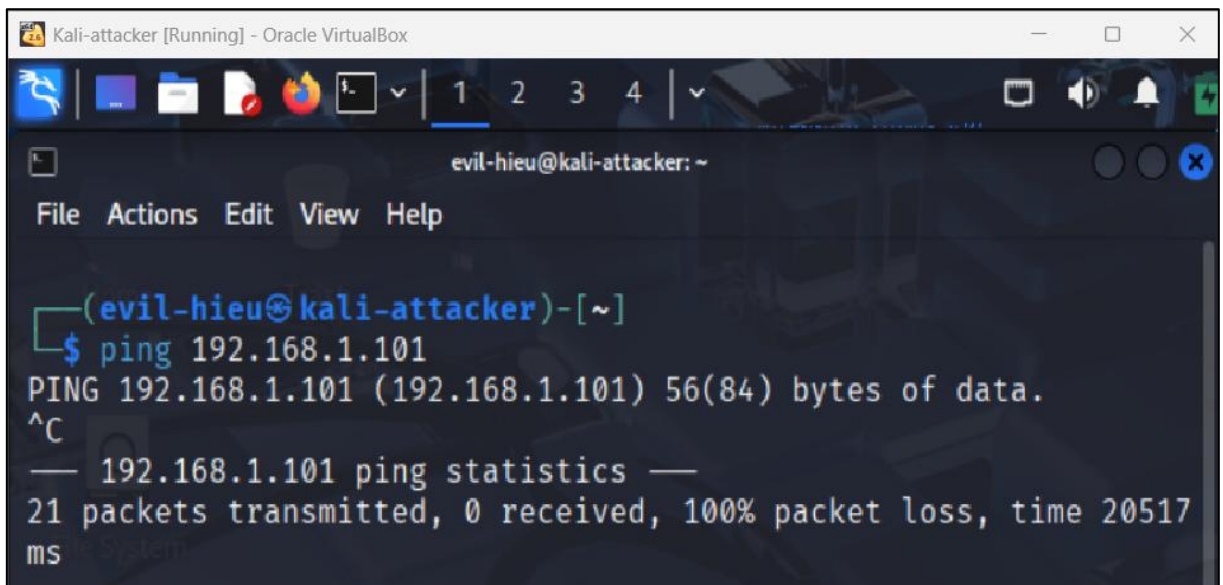


Figure 16: Kết quả lệnh ping không thể ping được sang victim

#### 4. Cấu hình port forwarding

Ta có thể cấu hình pfsense trên máy nội bộ bằng GUI vì pfsense cung cấp giao diện web tích hợp (WebGUI) cho phép quản trị viên truy cập và cấu hình firewall qua trình duyệt từ máy tính trong mạng nội bộ, miễn là bạn có quyền truy cập và địa chỉ IP của pfsense. Nên ta sẽ cấu hình pfsense ở máy nội bộ là máy ảo victim. Theo mặc định, tài khoản và mật khẩu lần lượt là *admin* và *pfsense*.

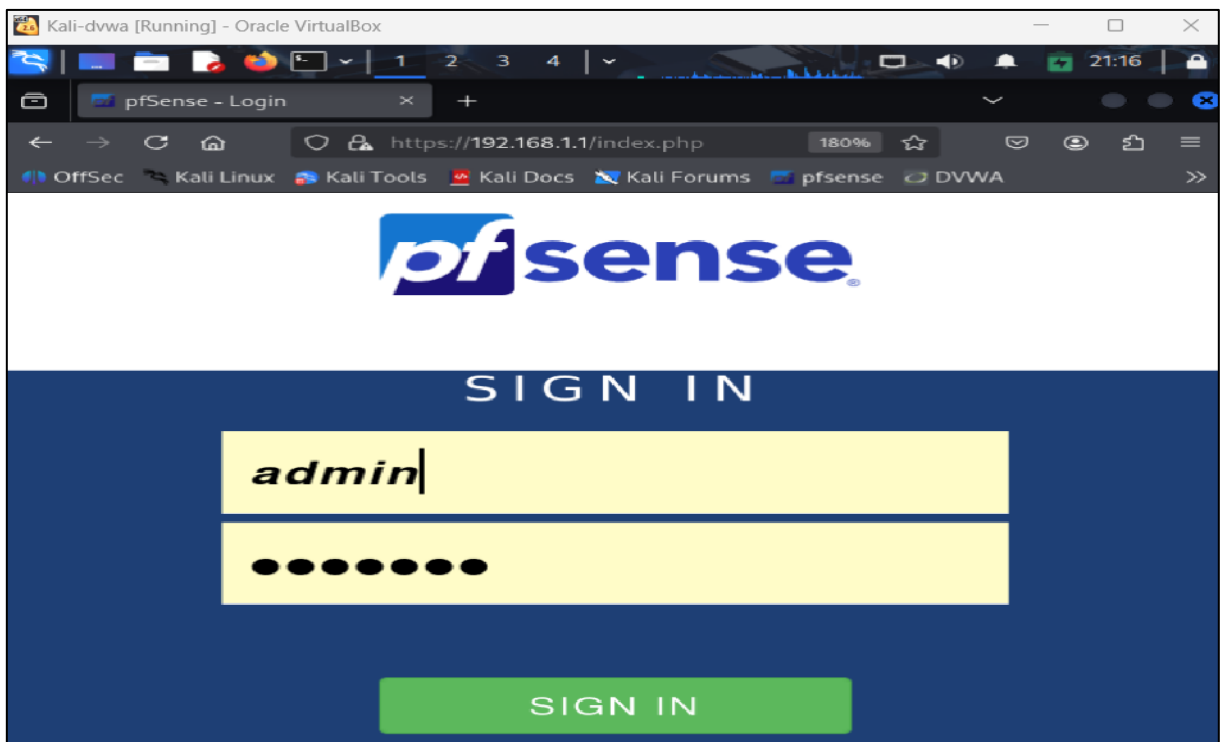


Figure 17: Giao diện GUI của pfsense trên máy ảo victim

Sau khi đăng nhập pfSense GUI thành công, ta sẽ xem rule chặn gói tin từ mạng ngoài bằng cách vào Firewall → Rules.

Hai rule này chỉ **chặn traffic từ WAN có địa chỉ IP thuộc dải private hoặc chưa được IANA cấp phát**, vậy nên khi attacker ping bị chặn vì pfSense mặc định Block private networks trên cổng WAN.

Muốn attacker ping qua pfSense tới victim, ta cần tắt tùy chọn này ở interface WAN hoặc tạo rule cho phép ICMP.

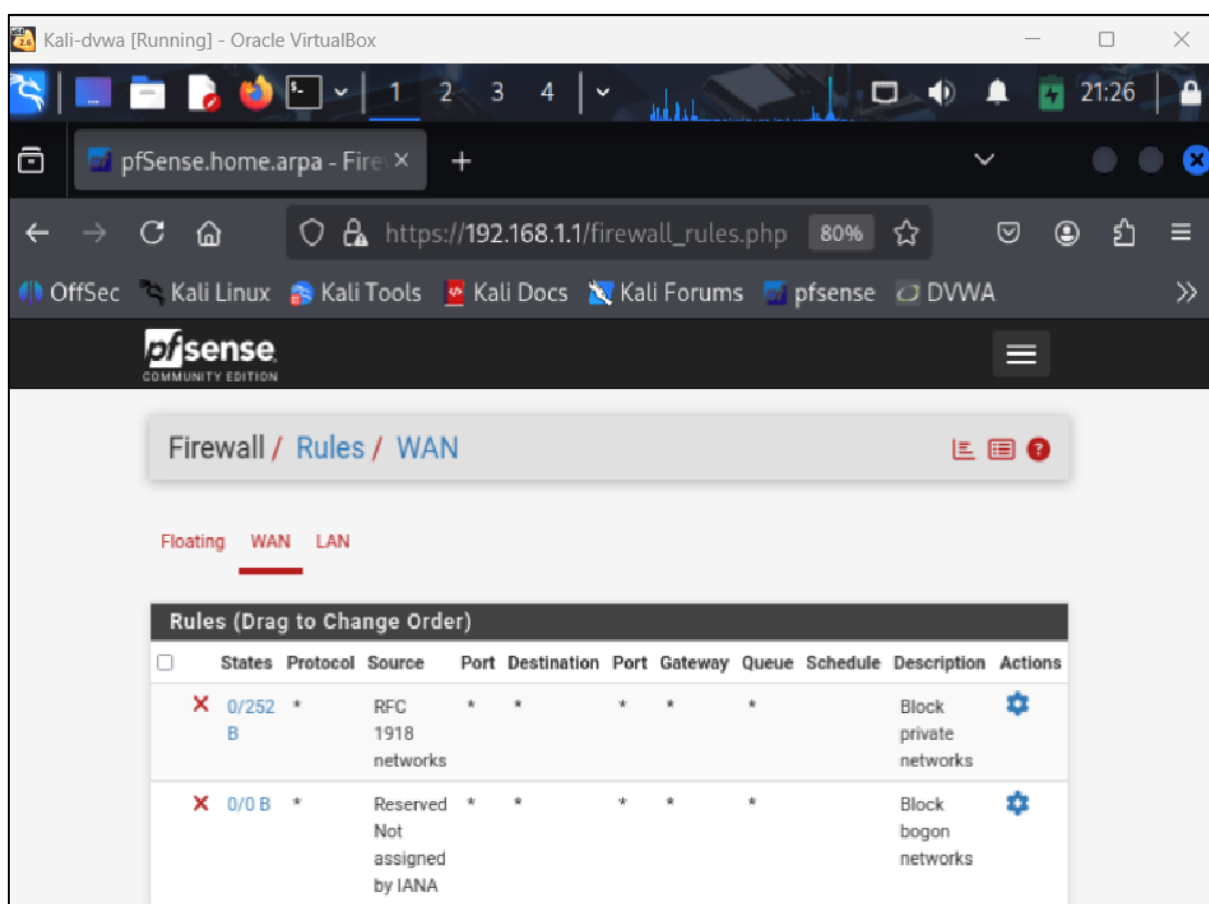


Figure 18: Rule mặc định chặn gói tin đi vào mạng nội bộ

Ta sẽ cấu hình Port Forward, ta lựa chọn Firewall → NAT. Từ đó bấm Add để thêm rule.



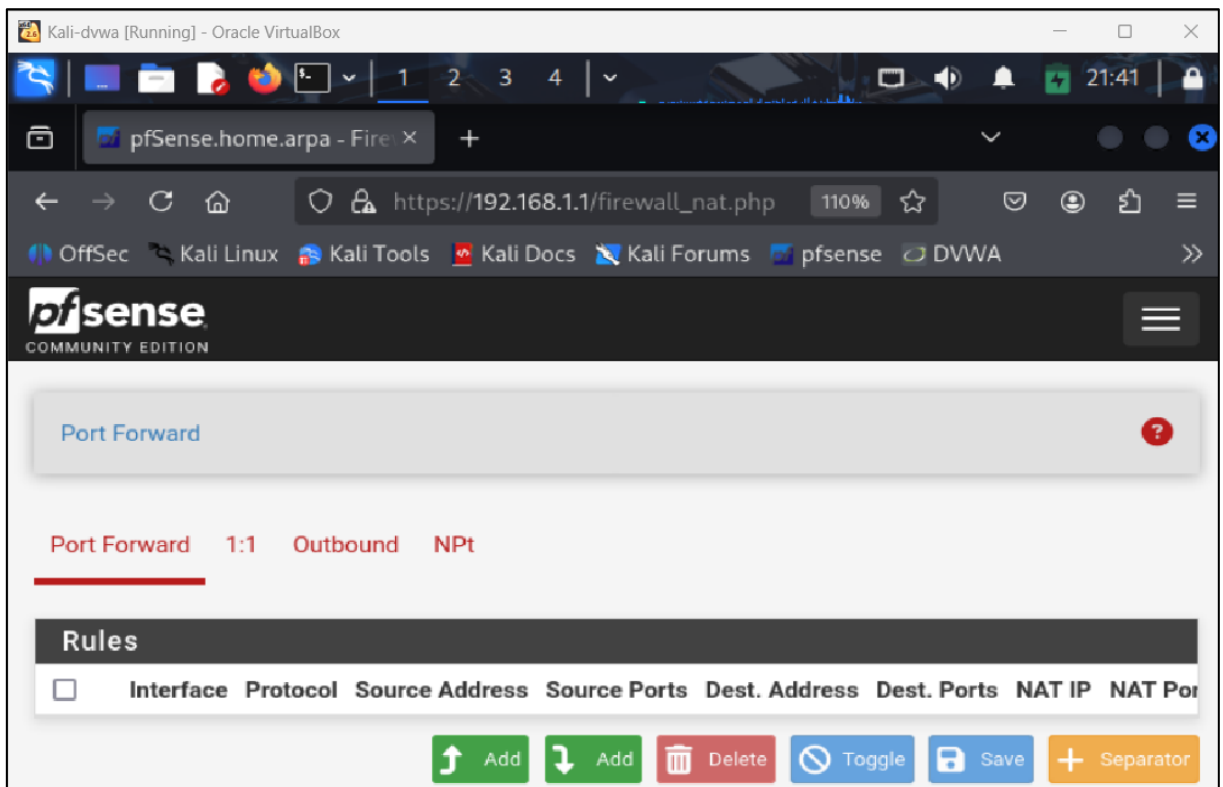


Figure 19: Cấu hình Port Forward

Ta muốn attacker ping được đến victim thì chọn Protocol sẽ là ICMP.

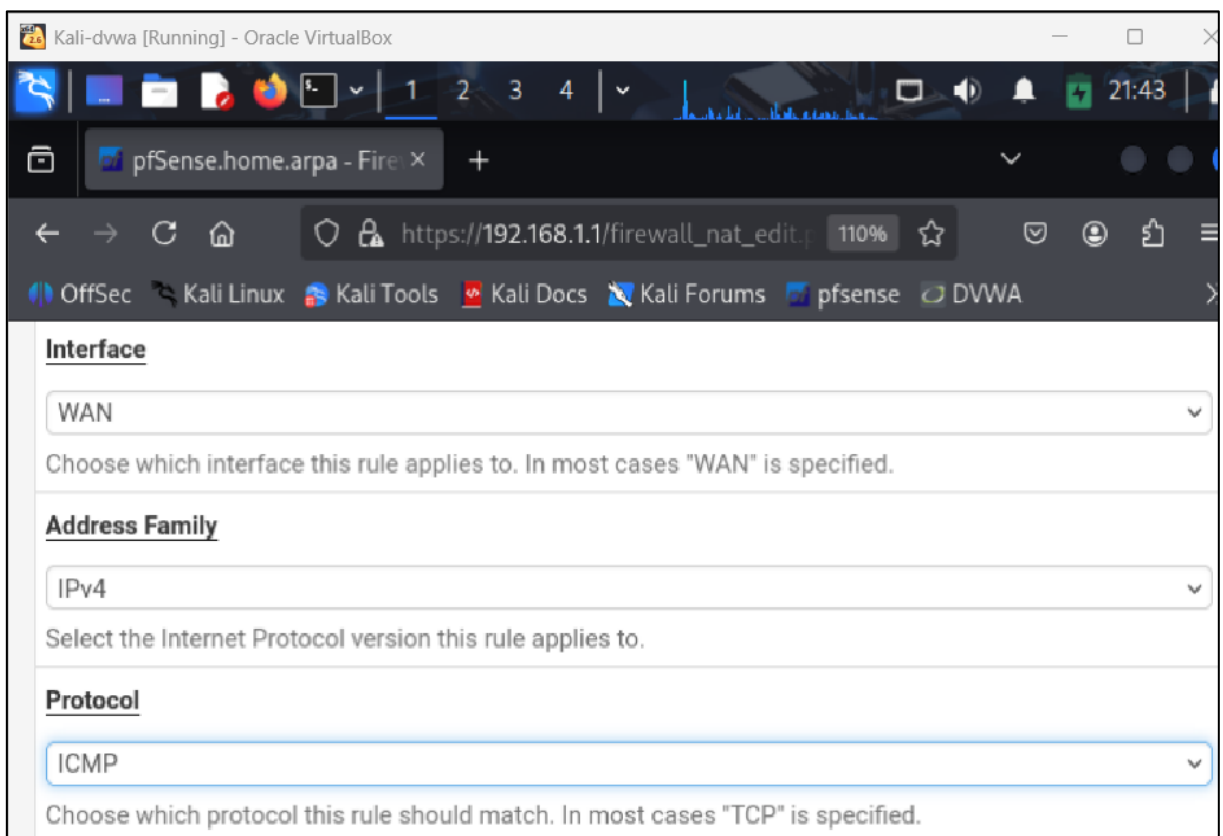


Figure 20: Chi tiết rule

Ta chọn Destination là LAN address vì victim nằm trong mạng nội bộ. Ngoài ra, để cho cụ thể ta sẽ cấu hình mọi gói tin đến từ interface WAN của pfsense sẽ được chuyển cho máy victim.

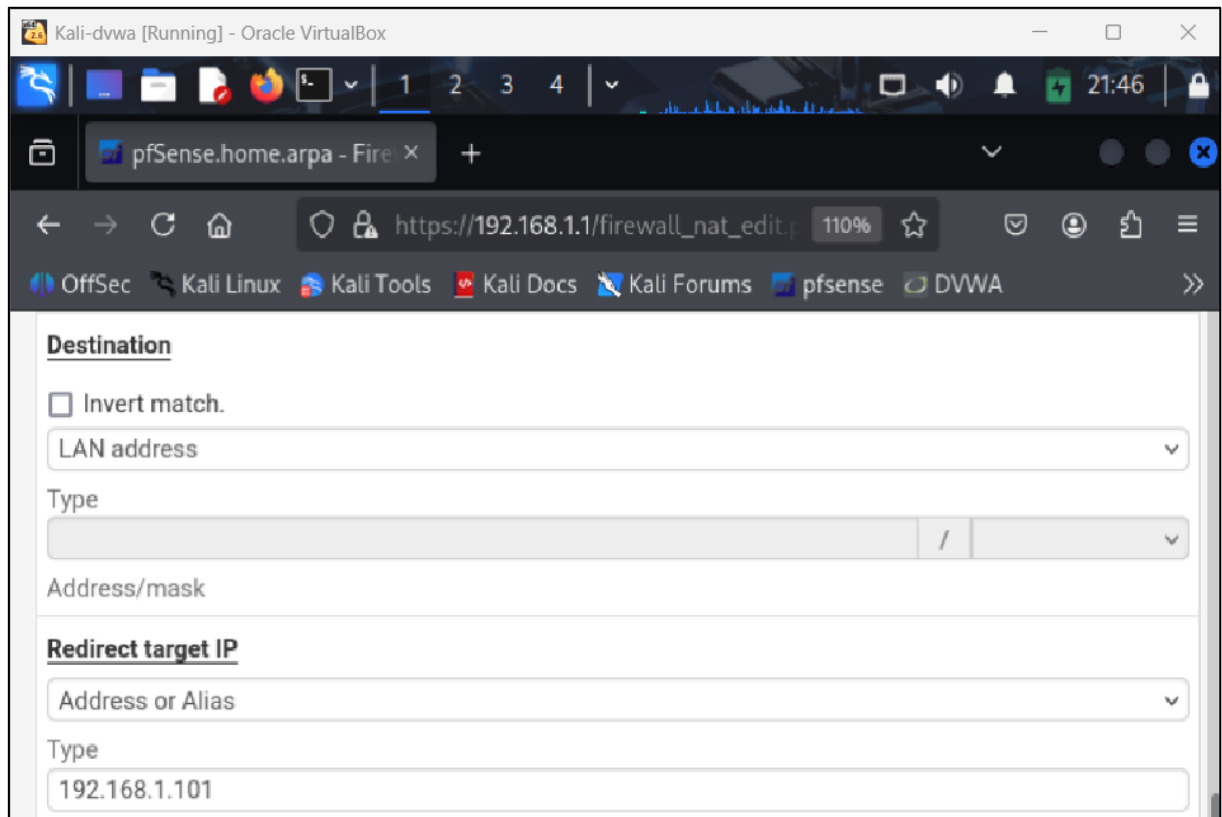


Figure 21: Cấu hình destination và redirected target IP

Sau đó ta có thể thêm description để quản trị viên có thể biết thêm thông tin khi pfSense phát hiện ra gói tin đến. Và ở lựa chọn “Filter rule association” sẽ tự động thêm rule cho ta ở Firewall → Rule. Cuối cùng, ta lưu rule lại.

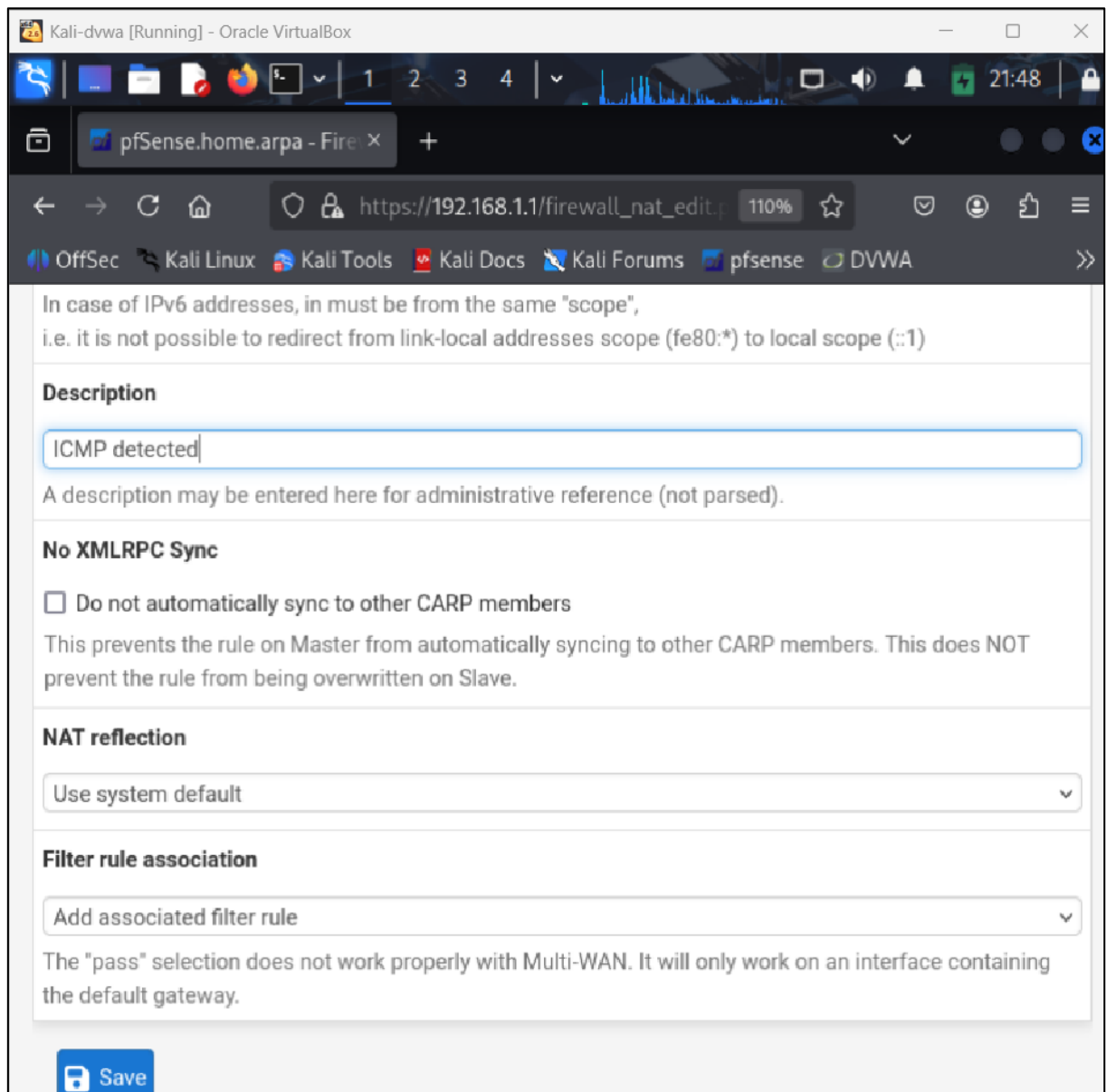


Figure 22: Thêm một số thông tin phụ rồi lưu

Ta sẽ sang Firewall → Rules, ta sẽ thấy pfsense sẽ tự động thêm rule cho ta.



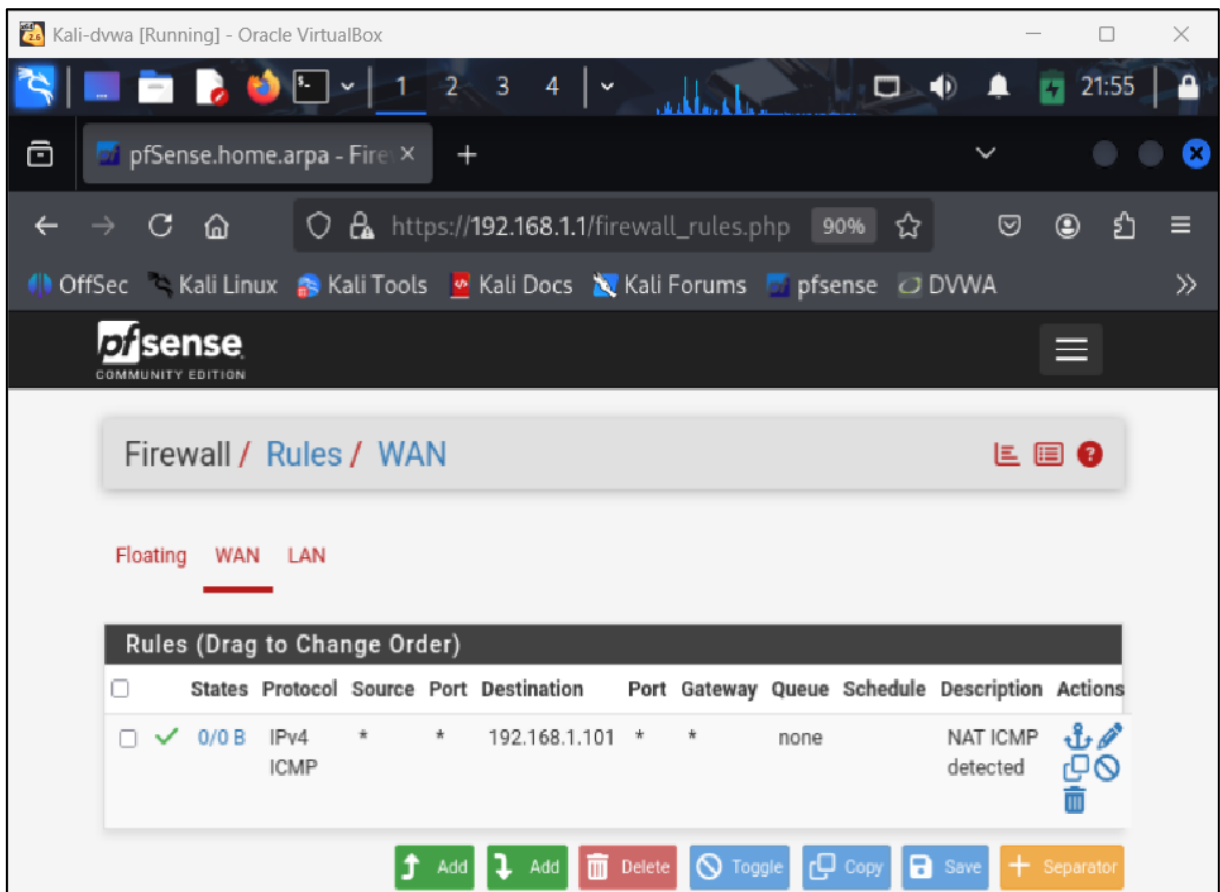


Figure 23: Rule cho phép gói tin ICMP đi qua firewall

## 5. Kiểm tra kết nối giữa các máy ảo

Ta kiểm tra kết nối từ attacker đến victim và ngược lại.

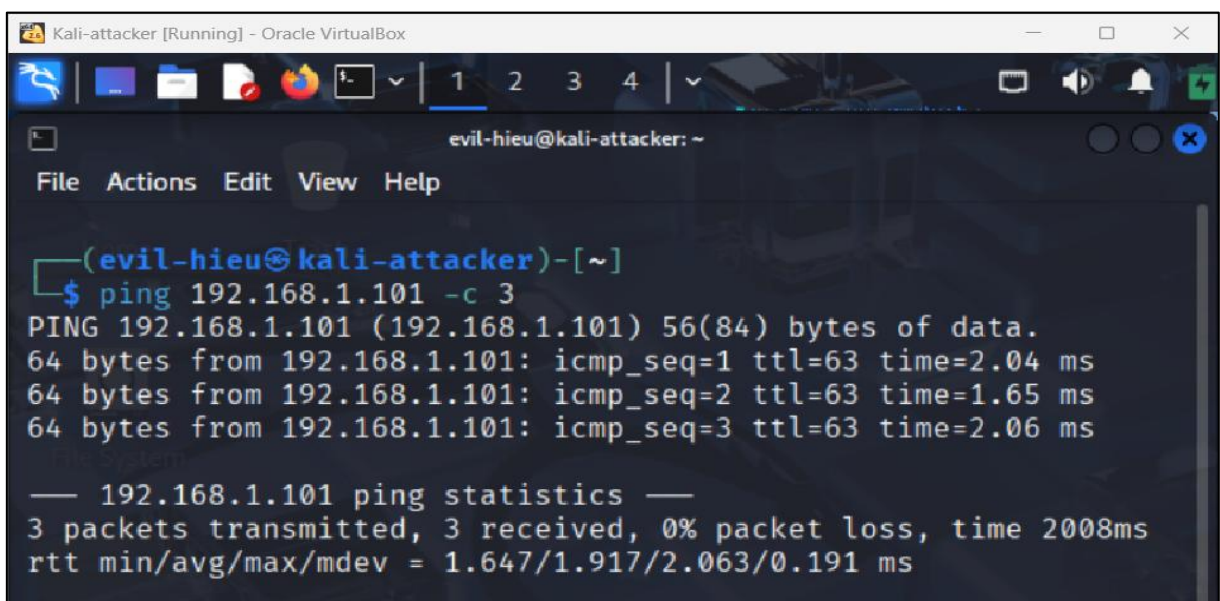
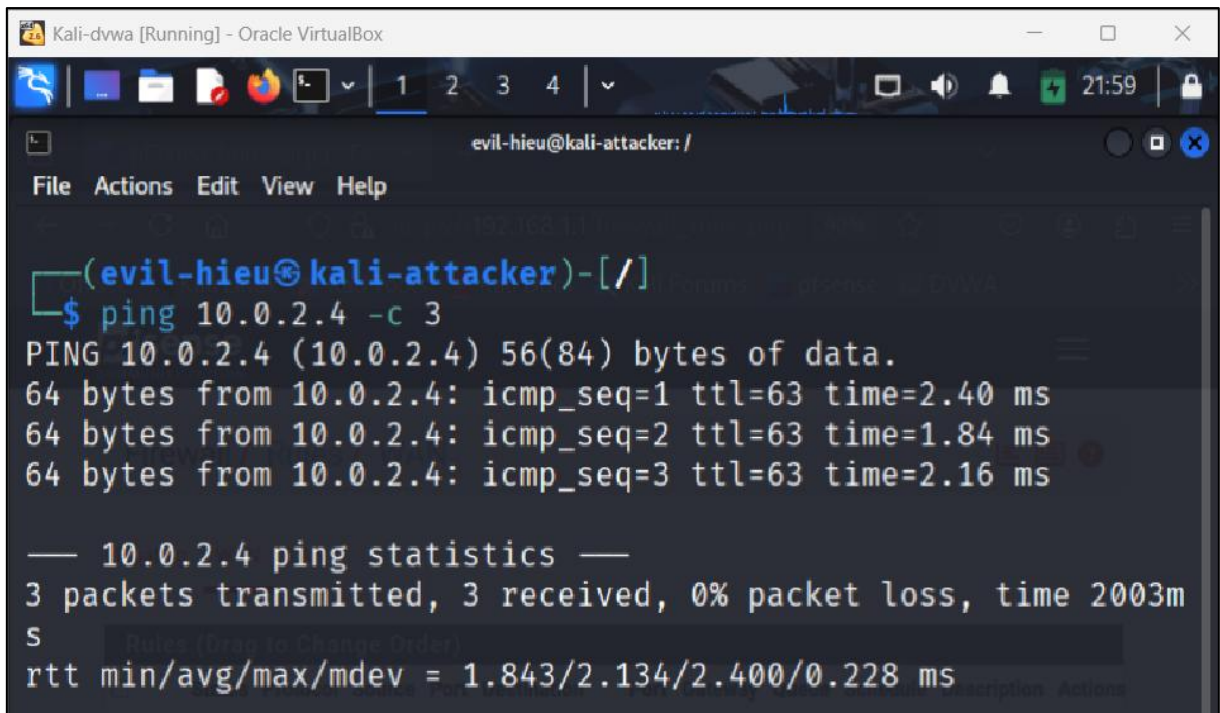


Figure 24: Lệnh ping từ attacker đến victim



```
(evil-hieu@kali-attacker)-[/]  
$ ping 10.0.2.4 -c 3  
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.  
64 bytes from 10.0.2.4: icmp_seq=1 ttl=63 time=2.40 ms  
64 bytes from 10.0.2.4: icmp_seq=2 ttl=63 time=1.84 ms  
64 bytes from 10.0.2.4: icmp_seq=3 ttl=63 time=2.16 ms  
  
— 10.0.2.4 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 1.843/2.134/2.400/0.228 ms
```

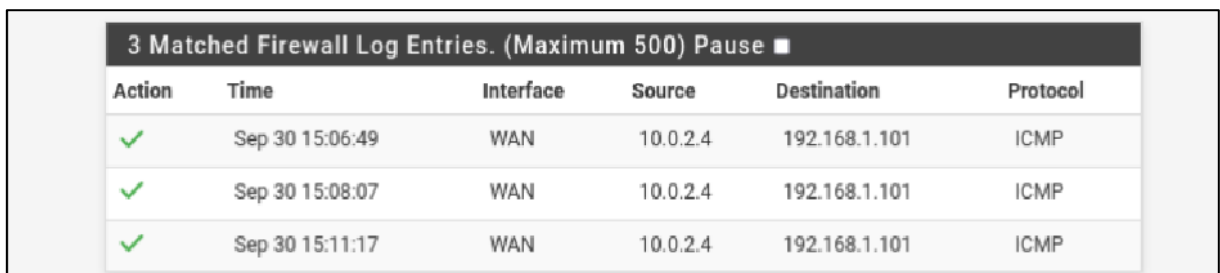
Figure 25: Lệnh ping từ victim đến attacker

Ta cũng có thể xem log của gói tin được ping từ attacker đến victim trước khi và sau khi thêm rule port forward trên pfsense.



×	Sep 30 14:26:06	WAN	(12011)	i 10.0.2.4	i+ 192.168.1.101	ICMP
×	Sep 30 14:26:07	WAN	(12011)	i 10.0.2.4	i+ 192.168.1.101	ICMP
×	Sep 30 14:26:08	WAN	(12011)	i 10.0.2.4	i+ 192.168.1.101	ICMP

Figure 26: Log trên pfsense trước khi thêm rule



3 Matched Firewall Log Entries. (Maximum 500) Pause						
Action	Time	Interface	Source	Destination	Protocol	
✓	Sep 30 15:06:49	WAN	10.0.2.4	192.168.1.101	ICMP	
✓	Sep 30 15:08:07	WAN	10.0.2.4	192.168.1.101	ICMP	
✓	Sep 30 15:11:17	WAN	10.0.2.4	192.168.1.101	ICMP	

Figure 27: Log trên pfsense sau khi thêm rule

#### IV. Đánh giá và kết luận

Qua quá trình cài đặt và cấu hình mô phỏng ba máy ảo (Attacker, pfsense, Victim), em đã:

- Hiểu được vai trò của pfsense như một firewall trung gian, kiểm soát luồng dữ liệu giữa Attacker và Victim.
- Nắm rõ cách cấu hình mạng trong VirtualBox (NAT, Internal Network) để đảm bảo các máy ảo có thể kết nối với nhau.
- Thực hành thiết lập các luật (rules) trong pfsense để cho phép hoặc chặn các gói tin ICMP, từ đó kiểm soát việc ping giữa các máy.
- Kiểm chứng thành công khả năng kết nối: Attacker có thể ping đến Victim thông qua pfsense khi đã cấu hình đúng.

Kết quả này giúp em rút ra kinh nghiệm rằng: việc kết nối mạng giữa các máy ảo không chỉ phụ thuộc vào cấu hình VirtualBox mà còn cần quản lý chặt chẽ bằng firewall rule trong pfsense. Đây là nền tảng quan trọng để triển khai các thí nghiệm về bảo mật mạng sau này, như tấn công và phòng thủ trong môi trường giả lập.