

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**

---



**BÀI BÁO CÁO THỰC HÀNH SỐ 5**

**MÔN THỰC TẬP CƠ SỞ**

**Tên sinh viên:** Ninh Chí Hường

**Mã sinh viên:** B20DCAT094

**Giảng viên hướng dẫn :** Th.s Ninh Thị Thu Trang

HÀ NỘI, THÁNG 3/2023

## Contents

I. Cơ sở lý thuyết .....	3
1. Mục đích.....	3
2. Tìm hiểu lý thuyết .....	3
II. Các bước thực hiện .....	4
1. Cấu hình topo mạng .....	4
2. Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP .....	7
3. Cài đặt cấu hình NAT pfsense firewall .....	10
4. Kiểm tra các cổng được phép truy cập trên mạng Internal .....	11
Tài liệu tham khảo .....	12

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

## **I. Cơ sở lý thuyết**

### **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. Tìm hiểu lý thuyết**

1. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware/Virtualbox

- Khi mới cài đặt VMware Workstation, mặc định phần mềm sẽ cài cho chúng ta 2 card mạng là một card VMnet0 kiểu là Bridged và một card VMnet8 kiểu là NAT. Ở đây ta có thêm một card mà ta cấu hình thêm là VMnet1 kiểu Host-only

- Để xem các card mạng đã có trong VMware Workstation ta chỉ cần bật VMware lên, chọn Edit => Virtual Network Editor Card bridge không có địa chỉ IP do nó sẽ sử dụng dải IP của máy thật.

- Card bridge, card này sử dụng chính card mạng thật của chúng ta để kết nối ra ngoài Internet (card ethernet hoặc wireless). Do đó khi sử dụng card mạng này IP của máy ảo sẽ cùng với dải IP của máy thật.

- Card NAT: card loại này cho phép máy ảo đi ra mạng vật lý bên ngoài Internet thông qua cơ chế NAT (Network Address Translation), lúc này lớp mạng bên trong máy ảo sẽ khác hoàn toàn với lớp mạng của card vật lý bên ngoài, hai mạng hoàn toàn tách biệt.

- Card Host-only: khi các máy ảo dùng card mạng loại này, nó sẽ không có kết nối vào mạng vật lý bên ngoài hay Internet thông qua máy thật, có nghĩa là mạng VMnet loại Host-only và mạng vật lý hoàn toàn tách biệt.

2. Tìm hiểu 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

=> 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.

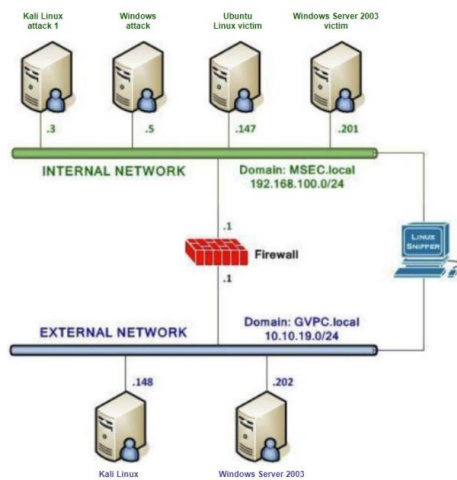
- Pfsense được cấu hình qua giao diện GUI trên nền web nên có thể quản lý một cách dễ dàng. Nó hỗ trợ lọc theo địa chỉ nguồn, đích, cũng như port nguồn hay port

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.<sup>4</sup>

## II. Các bước thực hiện

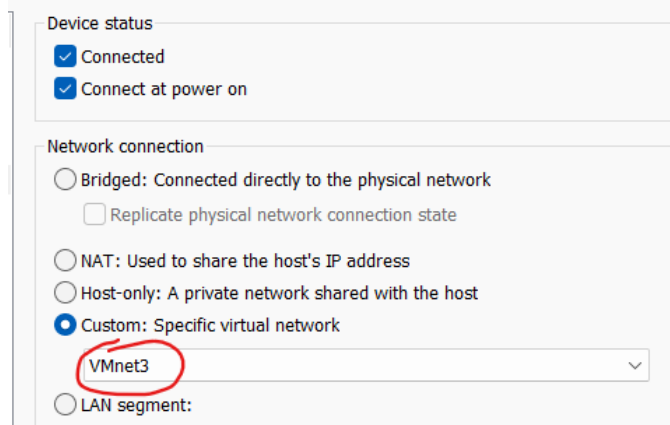
### 1. Cấu hình topo mạng



Máy Kali Linux attack 1 trong mạng Internal	IP: 192.168.100.3 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng Internal	IP: 192.168.100.201 Mật khẩu root: password
Máy Linux Victim trong mạng Internal	IP: 192.168.100.147 Mật khẩu root: password
Máy pfSense Firewall	IP: 10.10.19.1, 192.168.100.1 Mật khẩu: admin/pfsense
Máy Linux Attack trong mạng External	IP: 10.10.19.148 Mật khẩu root: password
Máy Windows Server 2003 Victim trong mạng External	IP: 10.10.19.202 Mật khẩu root: password

Cấu hình mạng :

Các máy mạng Internal sẽ chung card mạng Vmnet2. Các máy mạng External sẽ chung card mạng Vmnet 3, firewall sẽ dùng cả Vmnet2 và Vmnet3



+) IP máy Kali trong mạng Internal

```
(kali@B20AT094-HUong-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:fe4d:b329 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4d:b3:29 txqueuelen 1000 (Ethernet)
    RX packets 638 bytes 60616 (59.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 180 bytes 24394 (23.8 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 80 bytes 6384 (6.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 80 bytes 6384 (6.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

+) Máy Kali trong mạng Internal ping được 2 máy còn lại trong mạng

```
(kali@B20AT094-HUong-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=128 time=0.477 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=128 time=1.05 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=128 time=1.98 ms
^Z
zsh: suspended ping 192.168.100.147

(kali@B20AT094-HUong-Kali)-[~]
$ 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=64 time=0.420 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=64 time=1.08 ms
^Z
zsh: suspended ping 192.168.100.201
```

+) IP máy linux victim trong mạng Internal

```
huong@B20AT094-NinhChiHuong:~$ ifconfig
ens33    Link encap:Ethernet  HWaddr 00:0c:29:89:f9:f7
          inet addr:192.168.100.201  Bcast:192.168.100.255  Mask:255.255.0
          inet6 addr: fe80::de0:ff57:4460:feec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1531 errors:0 dropped:0 overruns:0 frame:0
          TX packets:326 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:192828 (192.8 KB)  TX bytes:49720 (49.7 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:349 errors:0 dropped:0 overruns:0 frame:0
          TX packets:349 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27063 (27.0 KB)  TX bytes:27063 (27.0 KB)
```

+) Máy Linux victim ping được 2 máy còn lại trong mạng

```
huong@B20AT094-NinhChiHuong:~$ 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=128 time=1.74 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=128 time=0.369 ms
^Z
[1]+  Stopped                  ping 192.168.100.147
huong@B20AT094-NinhChiHuong:~$ 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=0.644 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=1.08 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.398 ms
^Z
[2]+  Stopped                  ping 192.168.100.3
```

+) Tương tự với máy windows server trong mạng Internal

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::f427:7250:12b9:dbcd%5
    IPv4 Address. . . . . : 192.168.100.147
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>hostname & date
NinhChiHuong_B20DCAT094
The current date is: Thu 03/16/2023
Enter the new date: (mm-dd-yy)
```

```

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

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
^C
C:\Users\Administrator>ping 192.168.100.201

Pinging 192.168.100.201 with 32 bytes of data:
Reply from 192.168.100.201: bytes=32 time<1ms TTL=64
Reply from 192.168.100.201: bytes=32 time<1ms TTL=64
Reply from 192.168.100.201: bytes=32 time<1ms TTL=64
Reply from 192.168.100.201: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.100.201:
    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>^Z

```

+) Tương tự với máy Windows server trong mạng External

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

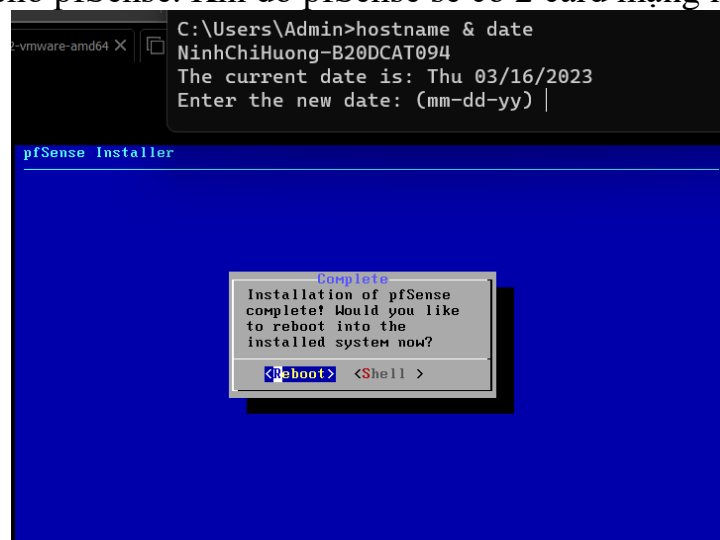
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1da9:7fce:9209:5567%5
    IPv4 Address. . . . . : 10.10.19.202
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\Administrator>

```

## Cài đặt máy pfSense Firewall:

- Ở mục Edit virtual machine settings, chọn Add, chọn Network Adapter để thêm một card mạng cho pfSense. Khi đó pfSense sẽ có 2 card mạng là vmnet2 và vmnet8



Setup IP cho các interface của firewall.

```
The IPv4 LAN address has been set to 192.168.100.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.100.1/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: b640e2dde0756887a0ed

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

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

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator 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: █
```

```
C:\WINDOWS\system. x + - □
C:\Users\Admin>hostname & date
NinhChiHuong-B20DCAT094
The current date is: Thu 03/16/2023
Enter the new date: (mm-dd-yy)
```

Sau khi cài đặt thành công, khởi động lại pfSense và bắt đầu cấu hình địa chỉ IP tĩnh cho pfSense.

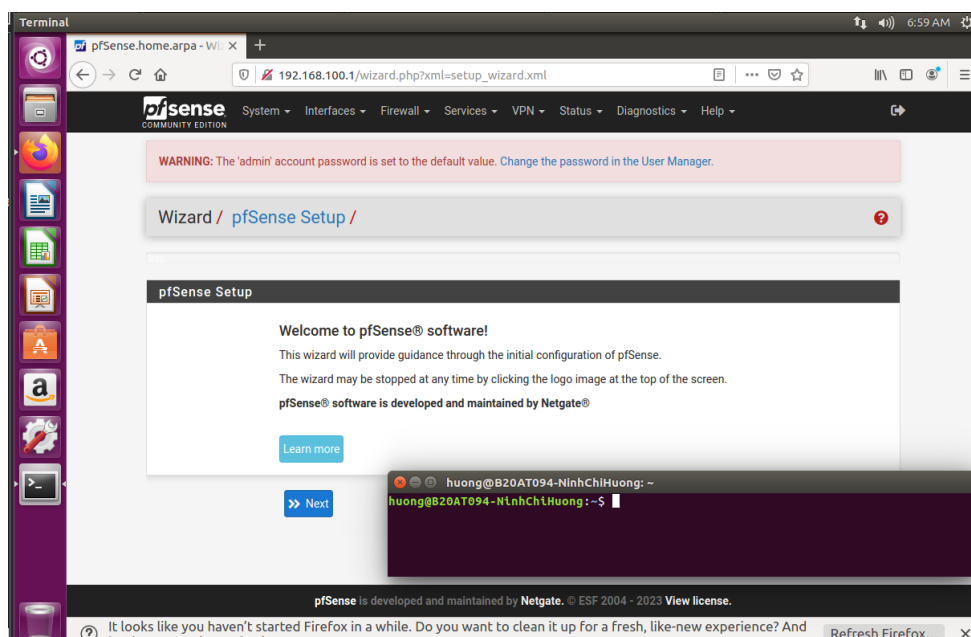
- Bấm 2 để mở tính năng cấu hình IP. Sau đó bấm 1 hoặc 2 để chọn WAN (mạng ngoài) hoặc LAN (mạng riêng).

- Điền địa chỉ IP của từng mạng: với WAN là 10.10.19.1, với LAN là 192.168.100.1

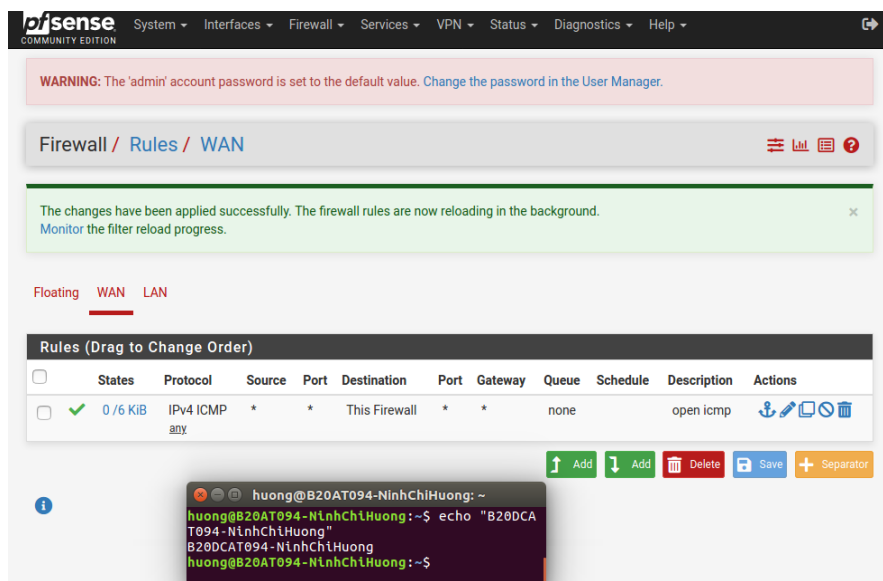
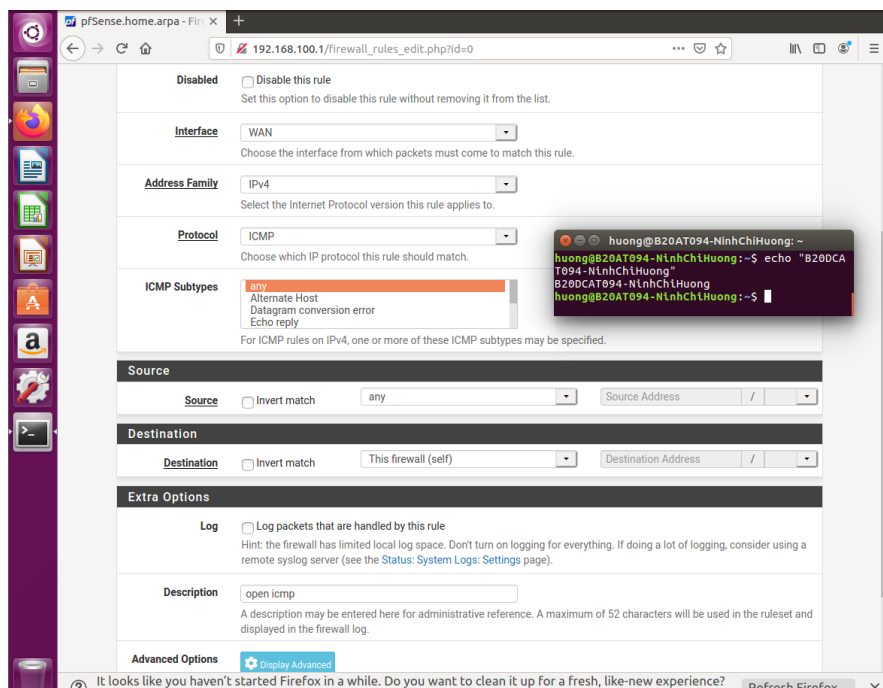
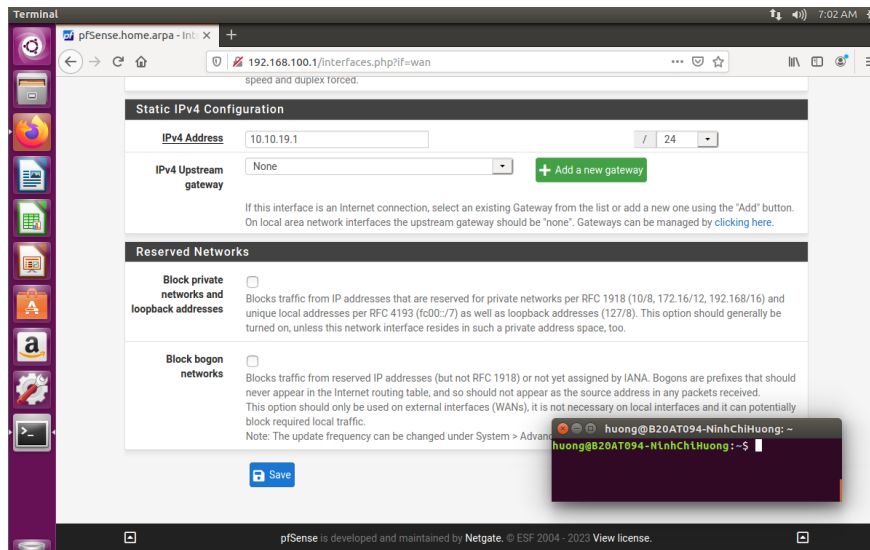
- Điền subnet là 24. Tắt DHCP Server trên pfSense vì đã có DHCP Server ảo của VMWare.

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

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



- Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1:



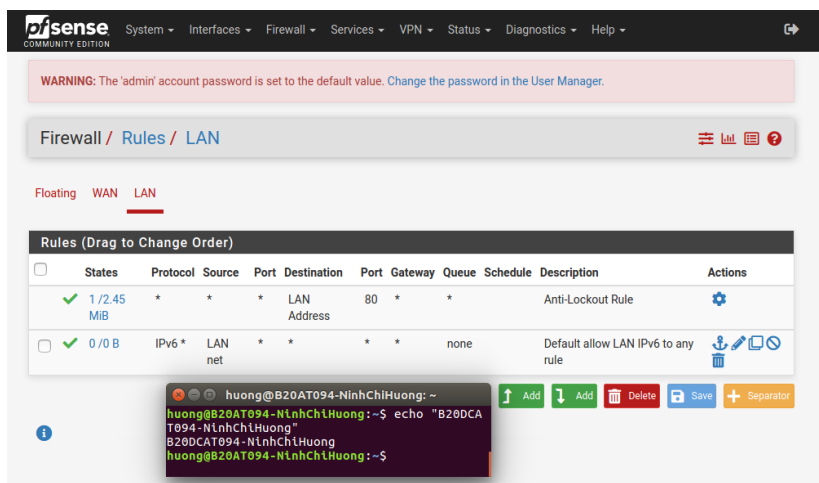


+)Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài

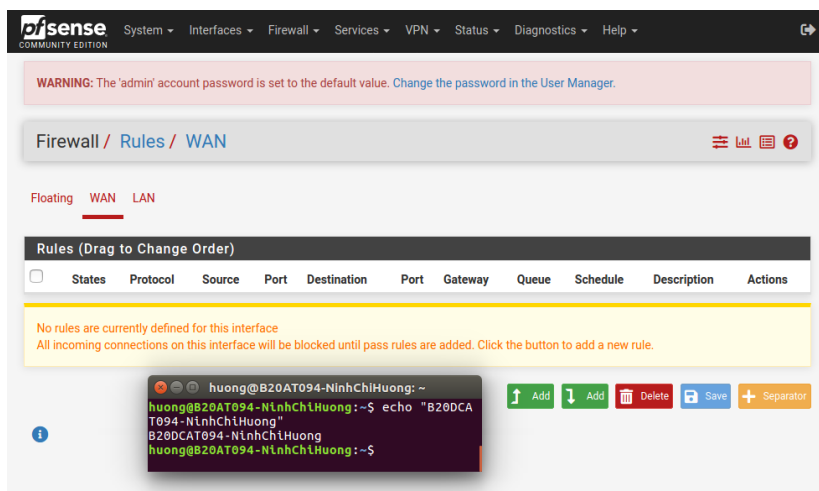
```
(kali@B20AT094-HUong-Kali)-[~]
$ ping 10.10.19.1
PING 10.10.19.1 (10.10.19.1) 56(84) bytes of data.
64 bytes from 10.10.19.1: icmp_seq=1 ttl=64 time=0.855 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.422 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.608 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=64 time=1.84 ms
64 bytes from 10.10.19.1: icmp_seq=5 ttl=64 time=0.420 ms
^Z
zsh: suspended ping 10.10.19.1
```

- Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?

+ Có 1 cổng TCP mở trên giao diện mạng trong của pfSense là cổng 80 đối với mạng Internal



Ngoài mạng External thì pfSense mặc định không mở cổng nào



### 3. Cài đặt cấu hình NAT pfsense firewall

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: [Display Advanced]

Destination: ☐ Invert match. WAN address  
Type: Address/mask

Destination port range: From port: SSH To port: SSH  
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: Single host 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.

- 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.

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.  
[Monitor the filter reload progress.](#)

Port Forward 1:1 Outbound NPT

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	22 (SSH)	192.168.100.147	22 (SSH)		

Legend: Pass Linked rule

Secure Shell

Secure Shell Server: ☒ Enable Secure Shell

SSHd Key Only: Password or Public Key  
When set to Public Key Only, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to Require Both Password and Public Key, the SSH access requires both a valid password and a valid public key. The default Password or Public Key setting allows either a valid password or a valid public key.

Allow Agent Forwarding: ☐ Enables ssh-agent forwarding support.

SSH port: 22  
Note: Leave this blank for the default of 22.

- 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?

```

(kali@B20AT094-HUong-Kali)-[~]
$ ssh huong@10.10.19.1
huong@192.168.14.152's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

UA Infra: Extended Security Maintenance (ESM) is not enabled.

0 updates can be applied immediately.

310 additional security updates can be applied with UA Infra: ESM
Learn more about enabling UA Infra: ESM service for Ubuntu 16.04 at
https://ubuntu.com/16-04

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

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.

huong@B20AT094-NinhChiHuong:~$ whoami
huong

```

```

huong@B20AT094-NinhChiHuong:~$ ifconfig
ens33    Link encap:Ethernet  HWaddr 00:0c:29:89:f9:f7
          inet addr:192.168.100.201  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::de0:ff57:4460:feec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5782 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2068 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3339928 (3.3 MB)  TX bytes:259515 (259.5 KB)

lo       Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:25695 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25695 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1761443 (1.7 MB)  TX bytes:1761443 (1.7 MB)

```

#### 4. Kiểm tra các cổng được phép truy cập trên mạng Internal:

```

huong@B20AT094-NinhChiHuong:~$ nmap 192.168.100.1

Starting Nmap 7.01 ( https://nmap.org ) at 2023-03-16 11:20 PDT
Nmap scan report for 192.168.100.1
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 4.75 seconds

```

## Tài liệu tham khảo

- VMWareVirtualNetwork Editor KB: <https://kb.vmware.com/s/article/1018697>
- pfSense Documentation: <https://docs.netgate.com/pfsense/en/latest/>
- Lab 7 pfsense firewall của CSSIA CompTIA Security+®
- Advanced Penetration Testing for Highly-Secured Environments  
Second Edition