

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

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

Họ và tên sinh viên:

Trần Đức Minh

Mã số sinh viên:

B20DCAT127

Họ và tên giảng viên:

TS. Đinh Trường Duy

## **I. Tìm hiểu lý thuyết:**

### **1. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng VMware:**

- VMware Workstation là một trình ảo hóa dựa trên máy tính, cung cấp khả năng chạy và mô phỏng nhiều hệ điều hành trên một máy tính. VMware Workstation đi kèm với rất nhiều tính năng kết nối mạng giúp ta tạo và quản lý các mạng riêng tư, chia sẻ hoặc cách ly bên trong VMware Workstation.
- VMware Workstation cũng cung cấp DHCP Server có thể dễ dàng sử dụng để phân phát địa chỉ IP cho các máy ảo chạy trên nó. Khi cài đặt VMware Workstation, có 3 mạng mặc định được tạo là VMnet0, VMnet1 và VMnet8. Chúng thuộc 3 loại mạng khác nhau đó là Bridged, Host-only và NAT.

+ Bridged Network: Máy ảo khi sử dụng mạng này sẽ hoạt động như một máy ảo độc lập kết nối đến switch hoặc router vật lý của người dùng. Máy ảo này sẽ trực tiếp lấy địa chỉ IP từ DHCP Server trong hạ tầng mạng người dùng và chúng có quyền truy cập đến các máy khác trong mạng và có thể liên kết với các máy khác trên mạng như một máy tính vật lý thông thường.

+ NAT Network: Đây là mạng mặc định được sử dụng khi người dùng tạo một máy ảo. Trong trường hợp này, máy ảo không có địa chỉ IP riêng trên mạng bên ngoài mà chúng sẽ nhận địa chỉ IP từ DHCP Server ảo của VMware. Thiết bị VMware NAT truyền dữ liệu mạng giữa một hoặc nhiều máy ảo và mạng bên ngoài. Nó xác định

các gói dữ liệu đến dành cho mỗi máy ảo và gửi chúng đến đích chính xác.

+ Host-only Network: Mạng này được sử dụng khi người dùng muốn tạo một mạng riêng hoàn toàn cô lập để máy ảo không thể tìm thấy mạng khác hoặc Internet. Host-only Network cung cấp kết nối mạng giữa máy ảo và máy chủ. sử dụng bộ chuyển đổi Ethernet ảo để máy chủ có thể tìm thấy.

## 2. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Virtualbox:

- Các máy ảo chạy trên VirtualBox có thể được kết nối với các mạng khác nhau.

- VirtualBox cung cấp nhiều chế độ mạng cho máy ảo. Mỗi máy ảo VirtualBox có thể sử dụng tối đa tám bộ chuyển đổi mạng (Adapter) ảo, mỗi bộ chuyển đổi trong số đó có nhiệm vụ là bộ điều khiển giao diện mạng (NIC). Bốn bộ chuyển đổi mạng ảo có thể được định cấu hình trong VirtualBox.

- Tất cả các bộ chuyển đổi mạng ảo có thể được cấu hình bằng lệnh VBoxManage modifyvm. VBoxManage là một công cụ quản lý dòng lệnh của VirtualBox có thể được sử dụng để định cấu hình tất cả cài đặt VirtualBox bao gồm cài đặt mạng VirtualBox.

- VirtualBox cung cấp nhiều chế độ mạng cho mỗi bộ chuyển đổi mạng ảo. Một số chế độ mạng đó là:

  - + Not attached (Không kết nối): Bộ chuyển đổi mạng ảo được cài đặt trong máy ảo, nhưng không có kết nối mạng.

+ NAT: Chế độ mạng này sử dụng cho bộ chuyển đổi mạng ảo theo mặc định. Hệ điều hành khách trên máy ảo có thể truy cập các máy chủ trong mạng cục bộ vật lý (LAN) bằng cách sử dụng thiết bị NAT ảo (Dịch địa chỉ mạng). Các mạng bên ngoài, bao gồm cả Internet, có thể truy cập được từ hệ điều hành khách. Khi chế độ NAT được sử dụng cho mạng VirtualBox, không thể truy cập máy khách từ máy chủ hoặc từ các máy khác trong mạng.

+ NAT Network: Chế độ này tương tự như chế độ NAT, nhưng nếu sử dụng chế độ mạng NAT cho nhiều máy ảo, chúng có thể giao tiếp với nhau qua mạng. Các máy ảo có thể truy cập các máy chủ khác trong mạng vật lý và có thể truy cập các mạng bên ngoài bao gồm cả Internet.

+ Bridged Adapter: Chế độ này được sử dụng để kết nối bộ chuyển đổi mạng ảo của máy ảo với mạng vật lý mà bộ chuyển đổi mạng vật lý của máy chủ VirtualBox được kết nối. Bộ chuyển đổi mạng ảo VM sử dụng giao diện mạng máy chủ để kết nối mạng.

+ Host-only Adapter: Chế độ mạng này được sử dụng để giao tiếp giữa máy chủ và khách. Một máy ảo có thể giao tiếp với các máy ảo khác và với máy chủ.

## **II. Nội dung thực hành:**

### **1. Cấu hình topo mạng:**

- Cấu hình địa chỉ IP cho máy Windows Server 2003 mạng Internal (IP 192.168.100.201), và mạng External (IP 10.10.19.202):

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

C:\Users\Administrator>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : MinhTD127-WSInternal
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-0C-29-35-EA-E2
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::1d52:e14a:3d46:a8a7%12(Preferred)
    IPv4 Address. . . . . : 192.168.100.201(Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
    DHCPv6 IAID . . . . . : 83889193
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-90-3D-70-00-0C-29-35-EA-E2
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>date
The current date is: Tue 02/28/2023
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

C:\Users\Administrator>
```

```
Administrator: Command Prompt
Windows IP Configuration

    Host Name . . . . . : MinhTD127-WSExternal
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . . :
    Description . . . . . : Intel(R) 82574L Gigabit Network Connection
    Physical Address. . . . . : 00-0C-29-8C-51-47
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    Link-local IPv6 Address . . . . . : fe80::e045:e295:bb6:353c%3(Preferred)
    IPv4 Address. . . . . : 10.10.19.202(Preferred)
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 10.10.19.1
    DHCPv6 IAID . . . . . : 50334761
    DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-90-3F-0E-00-0C-29-8C-51-47
    DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>date
The current date is: Tue 02/28/2023
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

C:\Users\Administrator>
```

- Cấu hình địa chỉ IP (10.10.19.148) cho Kali Linux External:

```
(kali@KaliExternal-MinhTD127)-[~]
$ ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.19.148 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::20c:29ff:fe68:9e79 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:68:9e:79 txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 276 (276.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9 bytes 726 (726.0 B)
    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 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@KaliExternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 03:23:33 AM EST

(kali@KaliExternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

(kali@KaliExternal-MinhTD127)-[~]
$
```

- Cấu hình địa chỉ IP (192.168.100.3) cho Kali Linux Internal:

```

(kali@KaliInternal-MinhTD127)-[~]
$ 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:fe14:a184 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:14:a1:84 txqueuelen 1000 (Ethernet)
    RX packets 12 bytes 811 (811.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 936 (936.0 B)
    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 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@KaliInternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 03:14:49 AM EST

(kali@KaliInternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

(kali@KaliInternal-MinhTD127)-[~]
$ █

```

- Cấu hình địa chỉ IP (192.168.100.147) cho Ubuntu Linux Internal:

```

b20dcat127-tdminh@ubuntu: ~
b20dcat127-tdminh@ubuntu:~$ ifconfig
ens33    Link encap:Ethernet HWaddr 00:0c:29:45:e3:35
          inet addr:192.168.100.147 Bcast:192.168.100.255 Mask:255.255.255.0
          inet6 addr: fe80::b18f:c13d:216b:cdb0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9254 (9.2 KB) TX bytes:7149 (7.1 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:3748 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3748 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:280704 (280.7 KB) TX bytes:280704 (280.7 KB)

b20dcat127-tdminh@ubuntu:~$ date
Tue Feb 28 00:25:41 PST 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$ █

```

- Cấu hình 2 interfaces cho pfSense: em0 có IP 10.10.19.1 cho mạng External, em1 có IP 192.168.100.1 cho mạng Internal:

```
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: 572bd84b2de5dfed53d9

*** Welcome to pfSense 2.6.0-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
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: TranDucMinh-B20DCAT127
```

- Thử nghiệm ping các máy trong mạng Internal với pfSense:

```
b20dcat127-tdminh@ubuntu: ~
b20dcat127-tdminh@ubuntu:~$ 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=0.443 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.206 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.198 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.198/0.282/0.443/0.114 ms
b20dcat127-tdminh@ubuntu:~$ date
Tue Feb 28 00:58:53 PST 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$
```



```
(kali@KaliInternal-MinhTD127)-[~]
$ 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=0.360 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=0.360 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.443 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.360/0.387/0.443/0.039 ms

(kali@KaliInternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 03:59:58 AM EST

(kali@KaliInternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

(kali@KaliInternal-MinhTD127)-[~]
$
```

- Thử nghiệm ping các máy Kali Linux và Ubuntu trong mạng Internal sử dụng Windows Server Internal:

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 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

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 = 0ms, Average = 0ms
Control-C
^C
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<1ms TTL=64

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

C:\Users\Administrator>

C:\Users\Administrator>date
The current date is: Tue 02/28/2023
Enter the new date: (mm-dd-yy)

C:\Users\Administrator>echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

C:\Users\Administrator>
```

- Thử nghiệm ping các máy Windows Server và Ubuntu trong mạng Internal sử dụng Kali Linux Internal:

```
(kali㉿KaliInternal-MinhTD127)-[~]
$ 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=128 time=0.906 ms
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=0.224 ms
64 bytes from 192.168.100.201: icmp_seq=3 ttl=128 time=0.401 ms
64 bytes from 192.168.100.201: icmp_seq=4 ttl=128 time=0.397 ms
^C
--- 192.168.100.201 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.224/0.482/0.906/0.255 ms

(kali㉿KaliInternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 03:50:18 AM EST

(kali㉿KaliInternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

(kali㉿KaliInternal-MinhTD127)-[~]
$ ping 192.168.100.147
PING 192.168.100.147 (192.168.100.147) 56(84) bytes of data.
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=1.02 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.402 ms
^C
--- 192.168.100.147 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.402/0.628/1.021/0.278 ms

(kali㉿KaliInternal-MinhTD127)-[~]
$ █
```

- Thử nghiệm ping các máy Windows Server và Kali Linux trong mạng Internal sử dụng Ubuntu Internal:

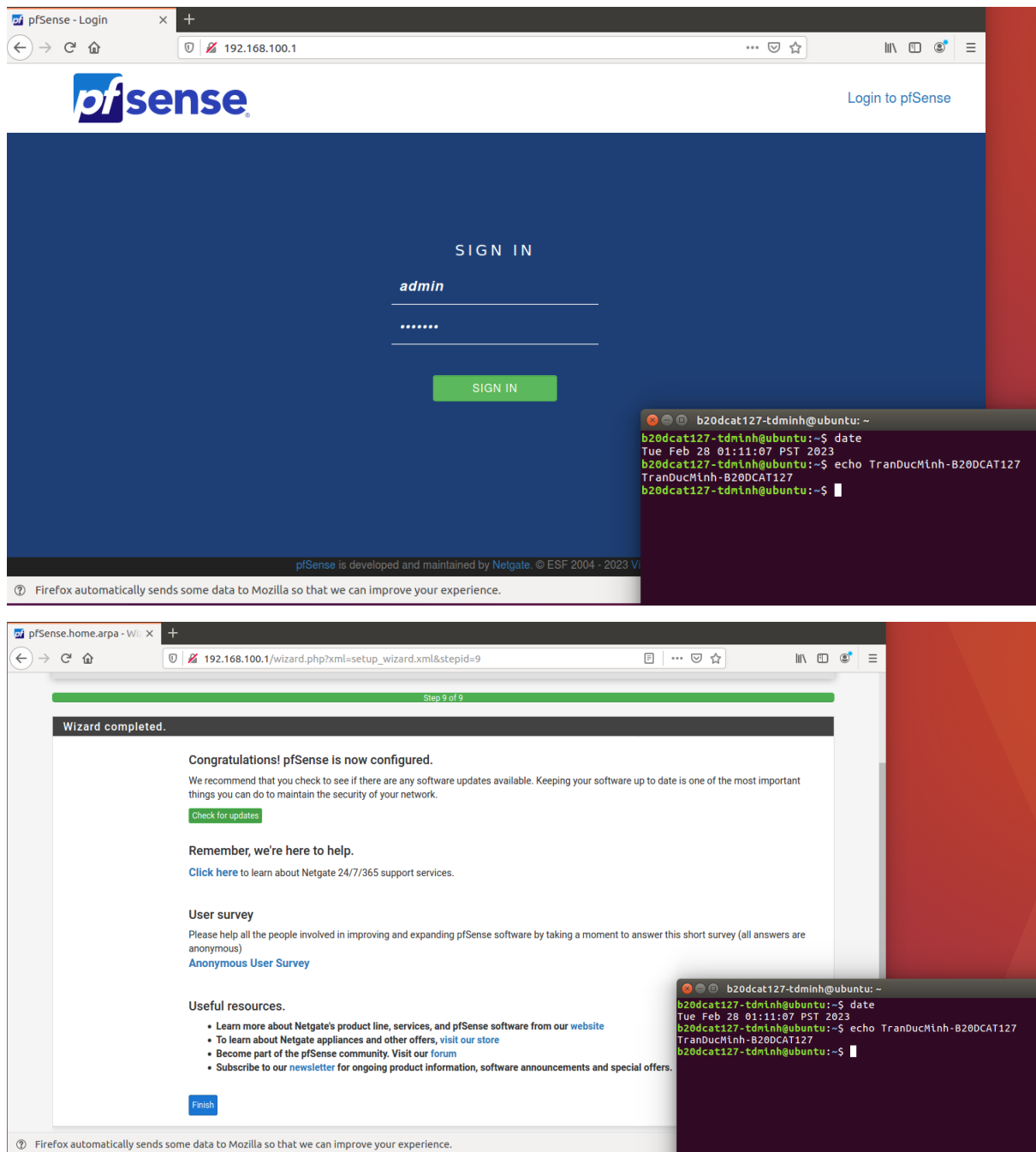
```
b20dcat127-tdminh@ubuntu: ~  
b20dcat127-tdminh@ubuntu:~$ ping 192.168.100.201  
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data.  
64 bytes from 192.168.100.201: icmp_seq=1 ttl=128 time=0.461 ms  
64 bytes from 192.168.100.201: icmp_seq=2 ttl=128 time=0.482 ms  
^C  
--- 192.168.100.201 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1009ms  
rtt min/avg/max/mdev = 0.461/0.471/0.482/0.024 ms  
b20dcat127-tdminh@ubuntu:~$ 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=0.325 ms  
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.398 ms  
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.293 ms  
^C  
--- 192.168.100.3 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2051ms  
rtt min/avg/max/mdev = 0.293/0.338/0.398/0.048 ms  
b20dcat127-tdminh@ubuntu:~$ date  
Tue Feb 28 00:57:31 PST 2023  
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127  
TranDucMinh-B20DCAT127  
b20dcat127-tdminh@ubuntu:~$
```

- Thử nghiệm ping máy Kali Linux trong mạng External sử dụng Windows Server External:

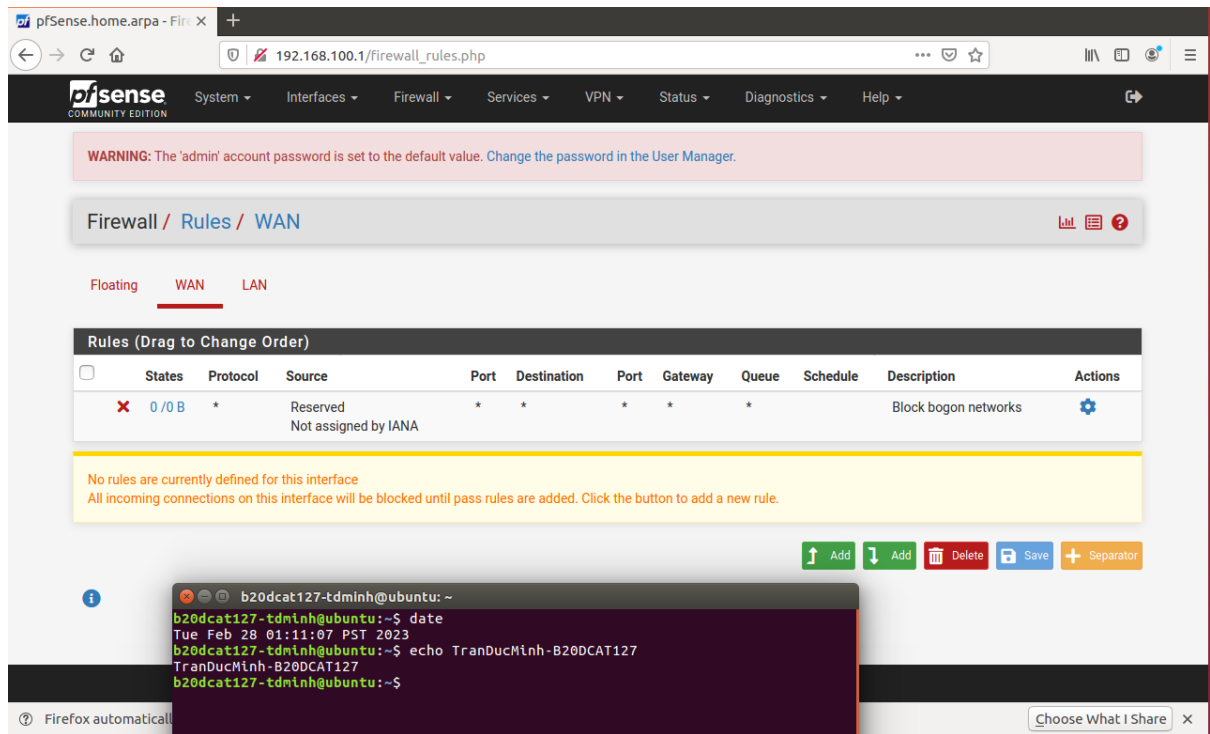
```
C:\Users\Administrator>date  
The current date is: Tue 02/28/2023  
Enter the new date: (mm-dd-yy)  
  
C:\Users\Administrator>echo TranDucMinh-B20DCAT127  
TranDucMinh-B20DCAT127  
  
C:\Users\Administrator>ping 10.10.19.148  
  
Pinging 10.10.19.148 with 32 bytes of data:  
Reply from 10.10.19.148: 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  
  
Ping statistics for 10.10.19.148:  
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 0ms, Maximum = 0ms, Average = 0ms  
Control-C  
^C  
C:\Users\Administrator>
```

## 2. Cài đặt cấu hình pfSense Firewall cho lưu lượng ICMP:

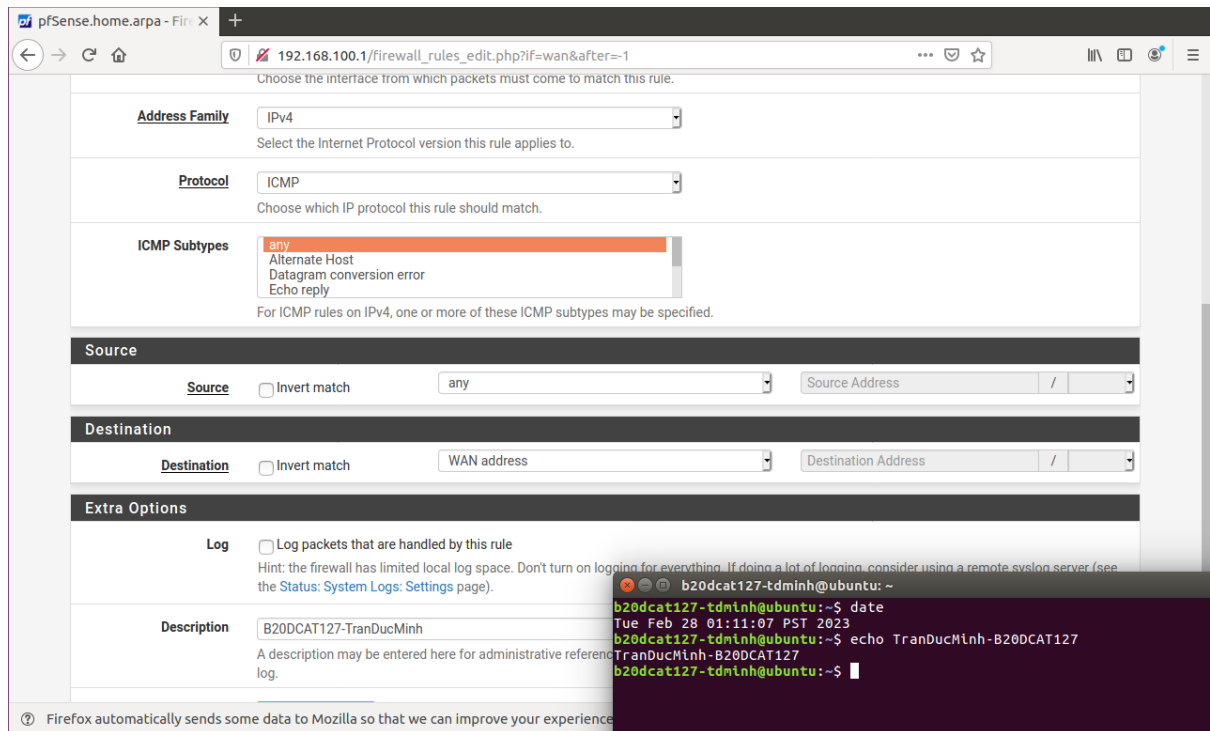
- Setup pfSense trên ứng dụng Web:



- Truy cập vào Firewall/Rule và Add để thêm luật cho pfSense:



- Thiết lập rule cấu hình ICMP cho phép các máy trong mạng Internal (LAN) ping được ra các máy ở mạng External (WAN), không cho phép ping vào trong mạng Internal:



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

```
(kali㉿KaliExternal-MinhTD127)-[~]
$ 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=0.375 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=64 time=0.324 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=64 time=0.352 ms
^C
--- 10.10.19.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.324/0.350/0.375/0.020 ms

(kali㉿KaliExternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 04:17:07 AM EST

(kali㉿KaliExternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAt127
TranDucMinh-B20DCAt127
```

- Trả lời câu hỏi:

+ Thử nghiệm quét bằng nmap cho thấy mặc định có 2 cổng

TCP mở trên giao diện mạng trong của pfSense:

```
(kali㉿KaliInternal-MinhTD127)-[~]
$ nmap -sV 192.168.100.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 04:20 EST
Nmap scan report for pfSense.home.arpa (192.168.100.1)
Host is up (0.0023s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
80/tcp    open  http   nginx

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.48 seconds

(kali㉿KaliInternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 04:20:37 AM EST

(kali㉿KaliInternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
```

+ Thử nghiệm quét bằng nmap cho thấy mặc định không có cổng TCP mở trên giao diện mạng ngoài của pfSense:

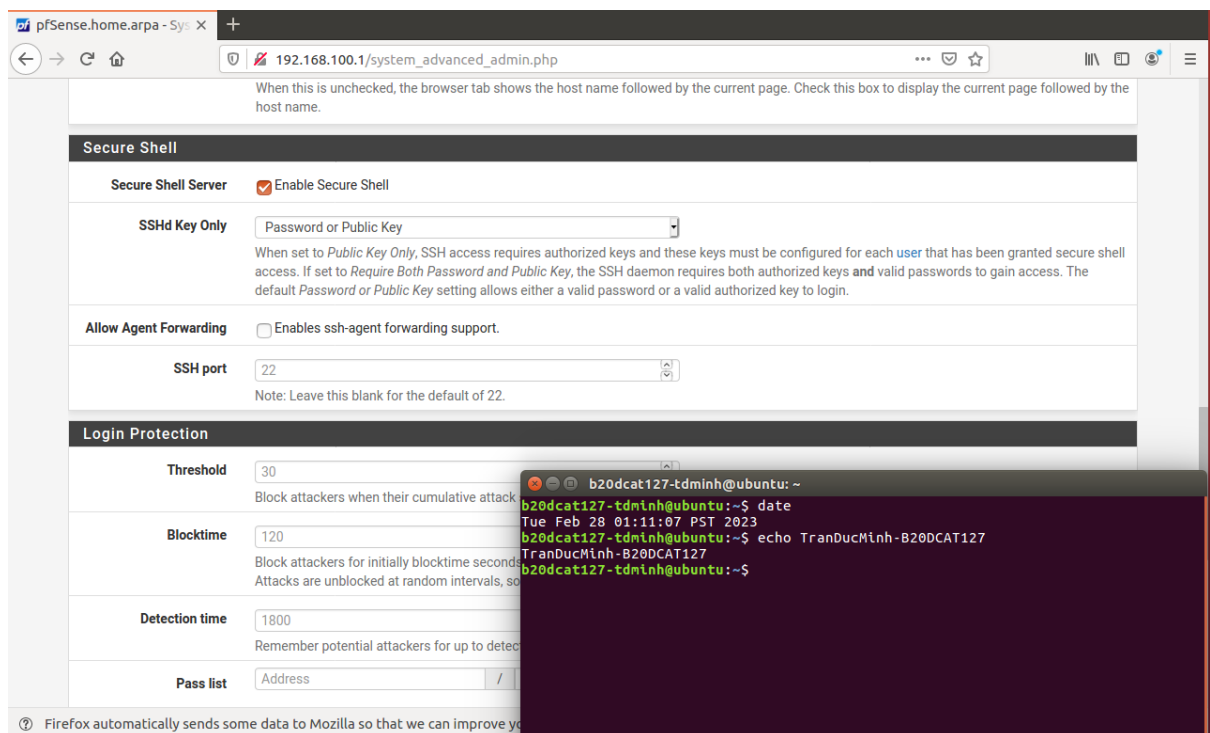
```
(kali㉿KaliExternal-MinhTD127)-[~]
$ date
Tue 28 Feb 2023 04:17:07 AM EST

(kali㉿KaliExternal-MinhTD127)-[~]
$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127

(kali㉿KaliExternal-MinhTD127)-[~]
$ nmap -sV 10.10.19.1
Starting Nmap 7.91 ( https://nmap.org ) at 2023-02-28 04:18 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.28 seconds
```

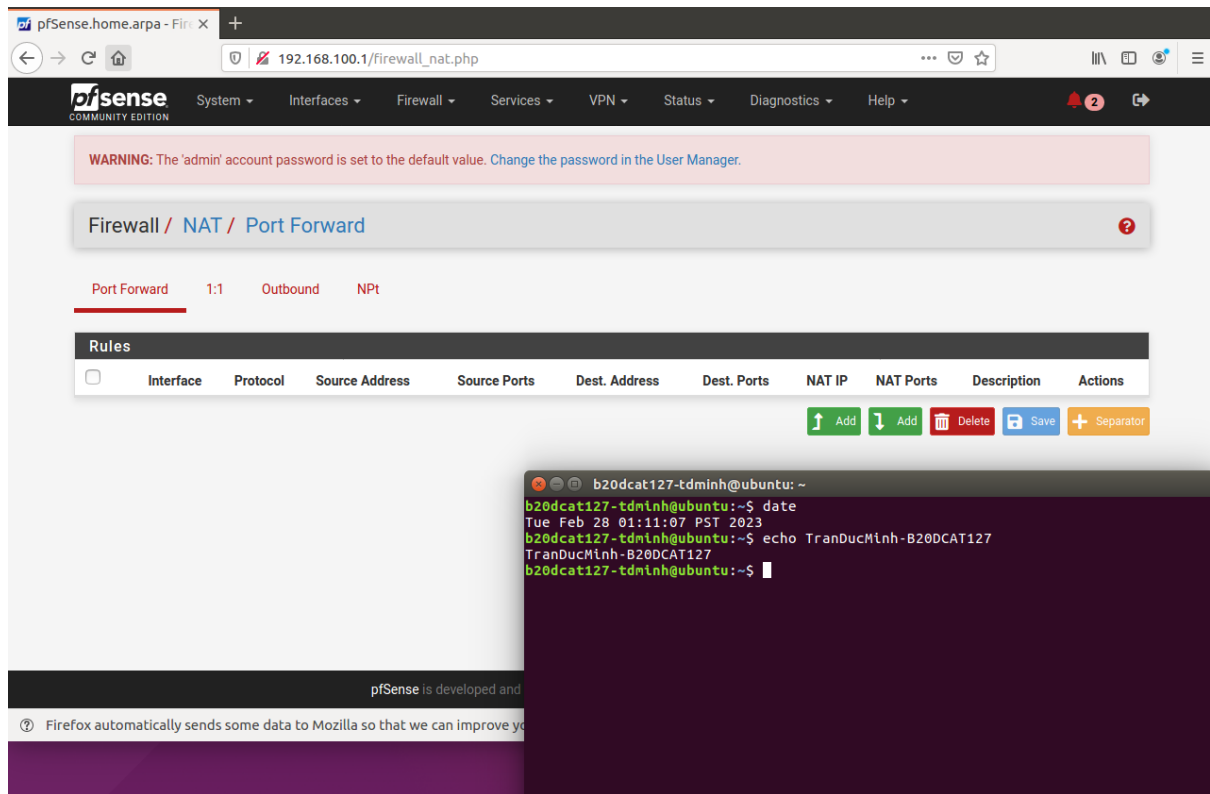
3. Cài đặt cấu hình pfSense Firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal:

- Trên máy Linux victim ở mạng trong, vào <http://192.168.100.1> để cấu hình NAT trên pfSense qua giao diện Web:

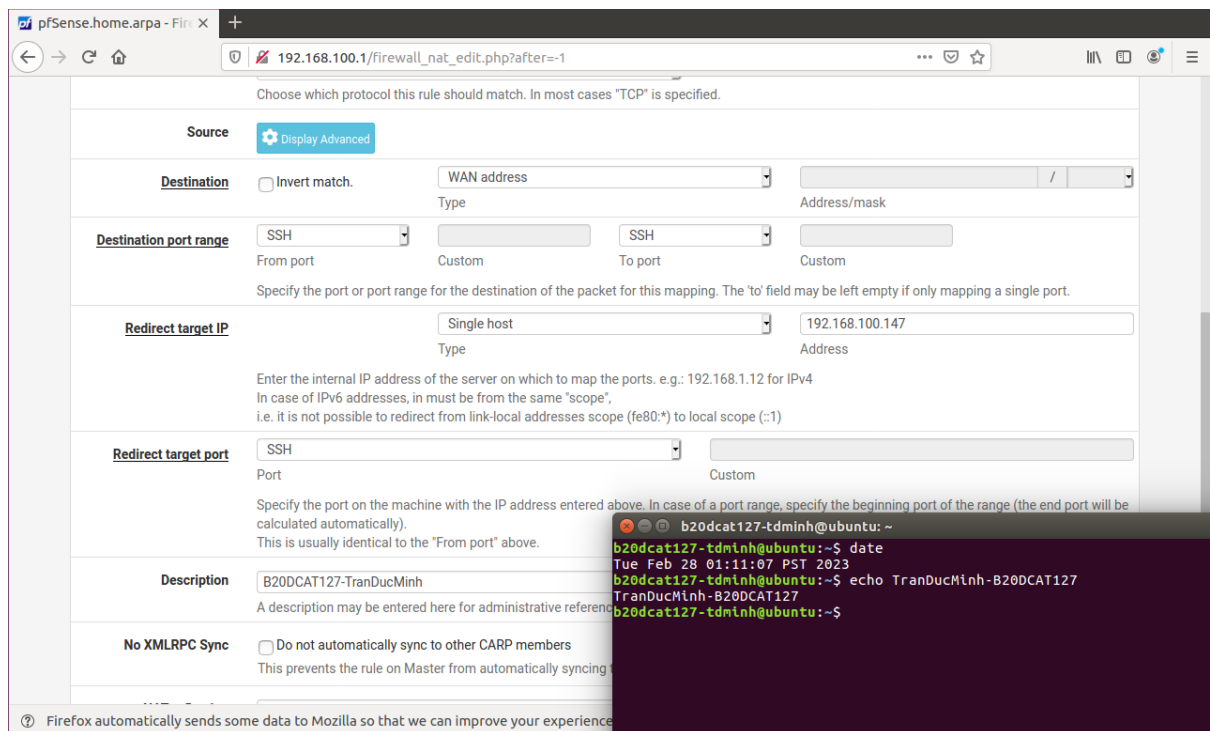


- Truy cập vào Firewall/Rule và Add trên Web quản lý của pfSense:





- 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:



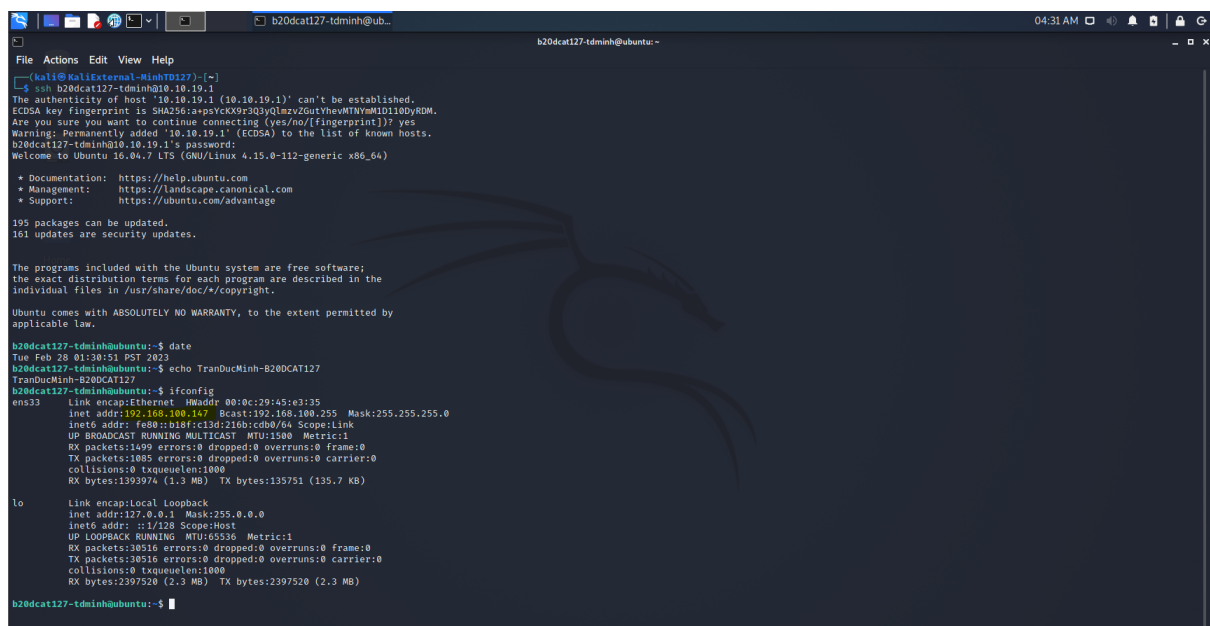


```

b20dcat127-tdminh@ubuntu:~$ date
Tue Feb 28 01:11:07 PST 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$ sudo ufw allow ssh
[sudo] password for b20dcat127-tdminh:
Rules updated
Rules updated (v6)
b20dcat127-tdminh@ubuntu:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Tue 2023-02-28 00:14:15 PST; 1h 13min ago
   Process: 2609 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
   Process: 2604 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Process: 960 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 972 (sshd)
   CGroup: /system.slice/ssh.service
           └─972 /usr/sbin/sshd -D

```

- Kiểm tra bằng cách truy cập SSH tới 10.10.19.1, sử dụng lệnh `ifconfig` kiểm tra được IP máy là 192.168.100.147:



```

b20dcat127-tdminh@ubuntu:~$ date
Tue Feb 28 01:11:07 PST 2023
b20dcat127-tdminh@ubuntu:~$ echo TranDucMinh-B20DCAT127
TranDucMinh-B20DCAT127
b20dcat127-tdminh@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 08:00:20:45:e3:35
    inet addr:192.168.100.147 Bcast:192.168.100.255 Mask:255.255.255.0
    inet6 addr: fe80::b18f:c134:2108::cd0/64 Scope:link
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
    RX packets:1499 errors:0 dropped:0 overruns:0 frame:0
    TX packets:1885 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:1393974 (1.3 MB)  TX bytes:135751 (135.7 KB)

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    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:30516 errors:0 dropped:0 overruns:0 frame:0
    TX packets:30516 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:2397520 (2.3 MB)  TX bytes:2397520 (2.3 MB)

b20dcat127-tdminh@ubuntu:~$

```

