Báo cáo bài thực hành số 5

Môn học

Thực tập cơ sở

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

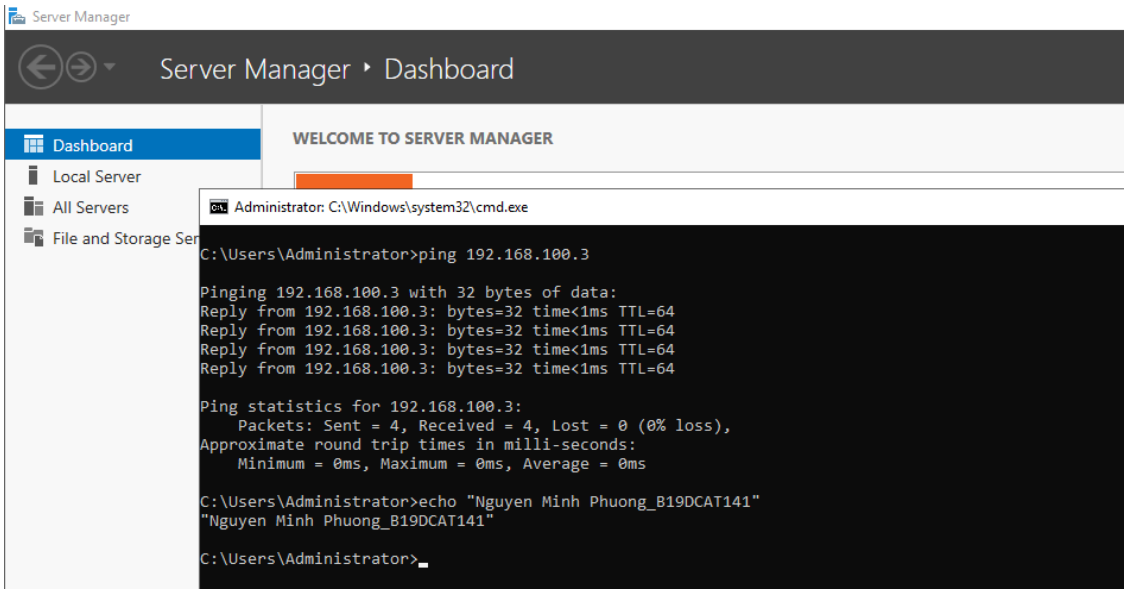
Mã SV: B19DCAT141

I. Lý thuyết :

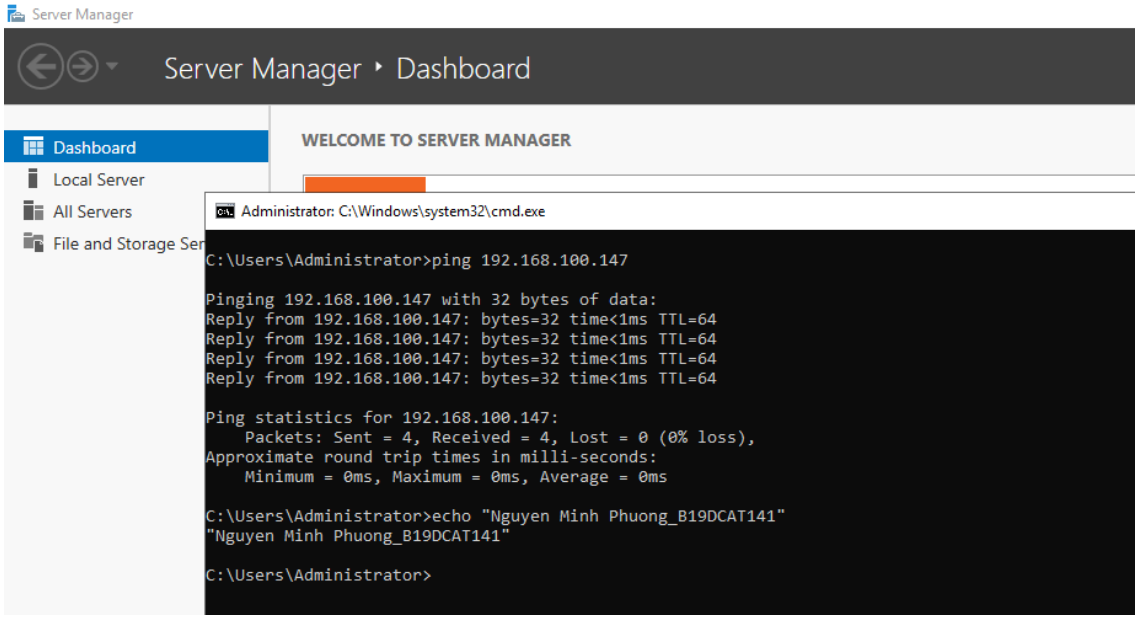
- Cấu hình mạng trong phần mềm mô phỏng Vmware
  + VMware là một phần mềm ảo hóa dùng cho desktop mạnh và phổ biến, đi kèm nhiều tính năng cho phép tạo và quản lý mạng riêng tư.
  + Các loại card mạng:
    - Bridge: card này sử dụng chính card mạng thật để kết nối ra ngoài Internet (card ethernet hoặc wireless). Do đó khi sử dụng card mạng này IP của máy ảo sẽ cùng với dải IP của máy thật.
    - Nat: sử dụng cách Nat địa chỉ IP của máy thật ra một địa chỉ khác cho máy ảo sử dụng. Card này cũng có thể kết nối ra bên ngoài Internet.
    - Host-only: hoàn toàn tách biệt với mạng thật. Card Hostonly chỉ có thể giao tiếp với máy ảo và các card Host-only trên các máy ảo khác.
- Pfsense
  + Là phần mềm định tuyến/tường lửa mã nguồn mở miễn phí dành cho máy tính dựa trên hệ điều hành FreeBSD.
  + Gồm tính năng gom nhóm các ports, host hoặc network khác nhau, tạo các rules để quản lý mạng bên trong Firewall.
  + Có thể cấu hình sử dụng cho DHCP server, DNS server, WiFi access point và VPN server, cho phép cài đặt các gói mã nguồn mở của bên thứ ba như Snort,..

II. Thực hành:

- Cấu hình topo mạng :
  + Máy Windows Server ping tới máy Kali Internal



+ Máy Windows Server ping tới máy Ubuntu Internal



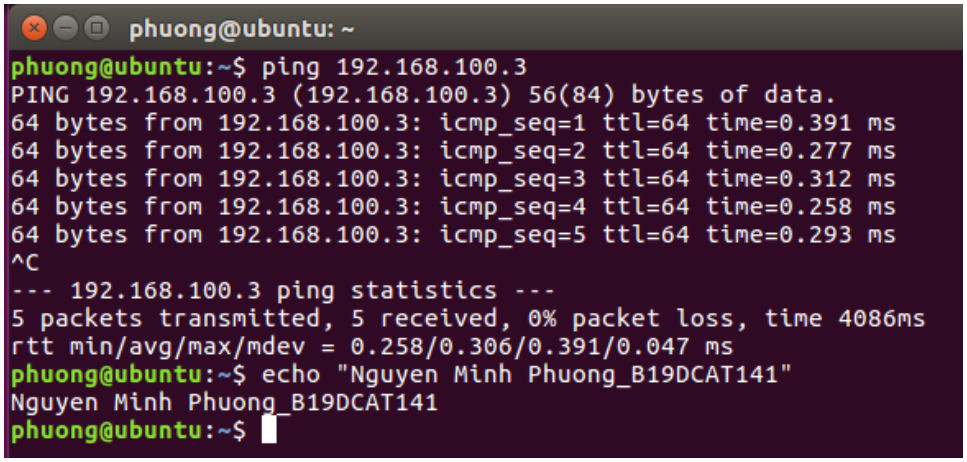
+ Máy Kali ping tới máy Ubuntu Internal

```
┌──(kali㉿b19dcat141-phuong-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=64 time=0.548 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=0.390 ms
64 bytes from 192.168.100.147: icmp_seq=3 ttl=64 time=0.310 ms
64 bytes from 192.168.100.147: icmp_seq=4 ttl=64 time=0.335 ms
64 bytes from 192.168.100.147: icmp_seq=5 ttl=64 time=0.284 ms
64 bytes from 192.168.100.147: icmp_seq=6 ttl=64 time=0.353 ms
64 bytes from 192.168.100.147: icmp_seq=7 ttl=64 time=0.258 ms
64 bytes from 192.168.100.147: icmp_seq=8 ttl=64 time=0.358 ms
^C
── 192.168.100.147 ping statistics ──
8 packets transmitted, 8 received, 0% packet loss, time 7146ms
rtt min/avg/max/mdev = 0.258/0.354/0.548/0.083 ms

┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ echo "Nguyen Minh Phuong_B19DCAT141"
Nguyen Minh Phuong_B19DCAT141
```

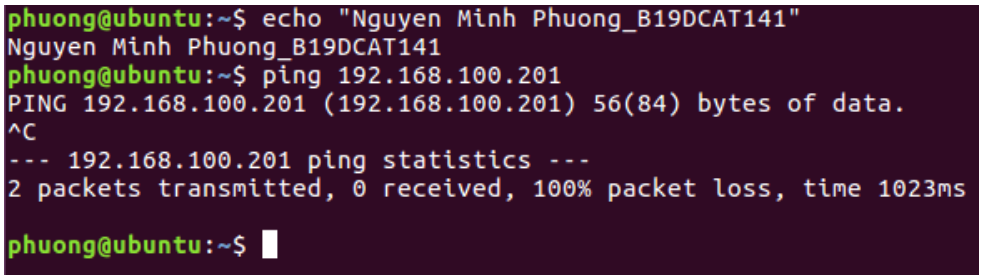
+ Máy Kali ping tới máy Windows Server Internal

```
┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ echo "Nguyen Minh Phuong_B19DCAT141"
Nguyen Minh Phuong_B19DCAT141

┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$ ping 192.168.100.201
PING 192.168.100.201 (192.168.100.201) 56(84) bytes of data.
^C
── 192.168.100.201 ping statistics ──
8 packets transmitted, 0 received, 100% packet loss, time 7169ms


┌──(kali㉿b19dcat141-phuong-kali)-[~]
└─$
```

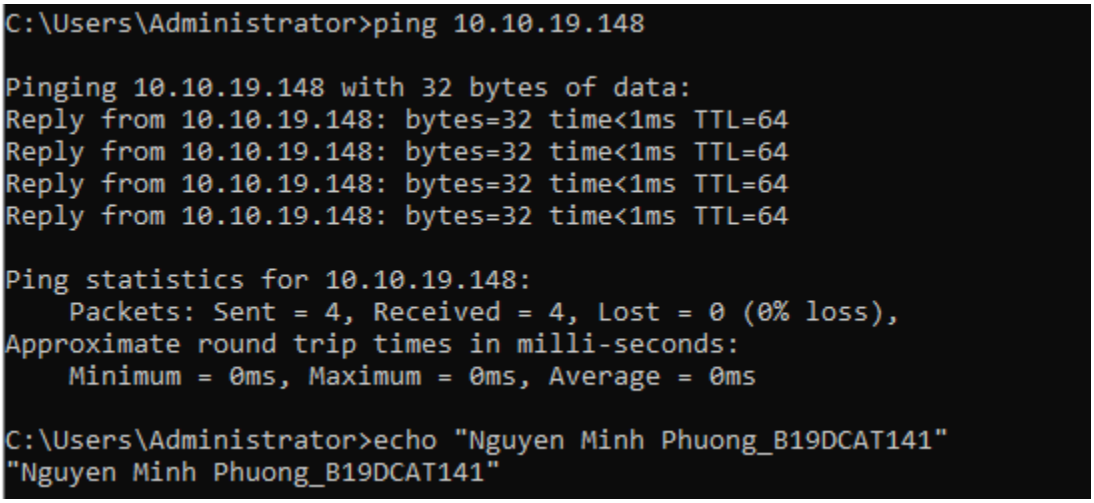
+ Máy Ubuntu ping tới máy Kali Internal



+ Máy Ubuntu ping tới máy Windows Server Internal



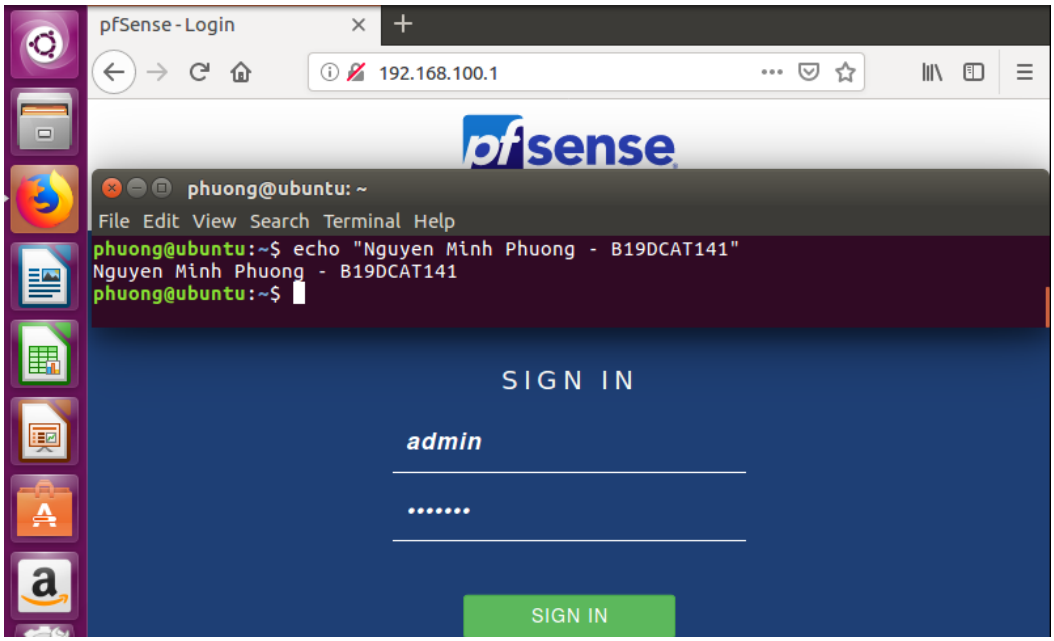
+ Máy Windows Server ping tới máy Kali External



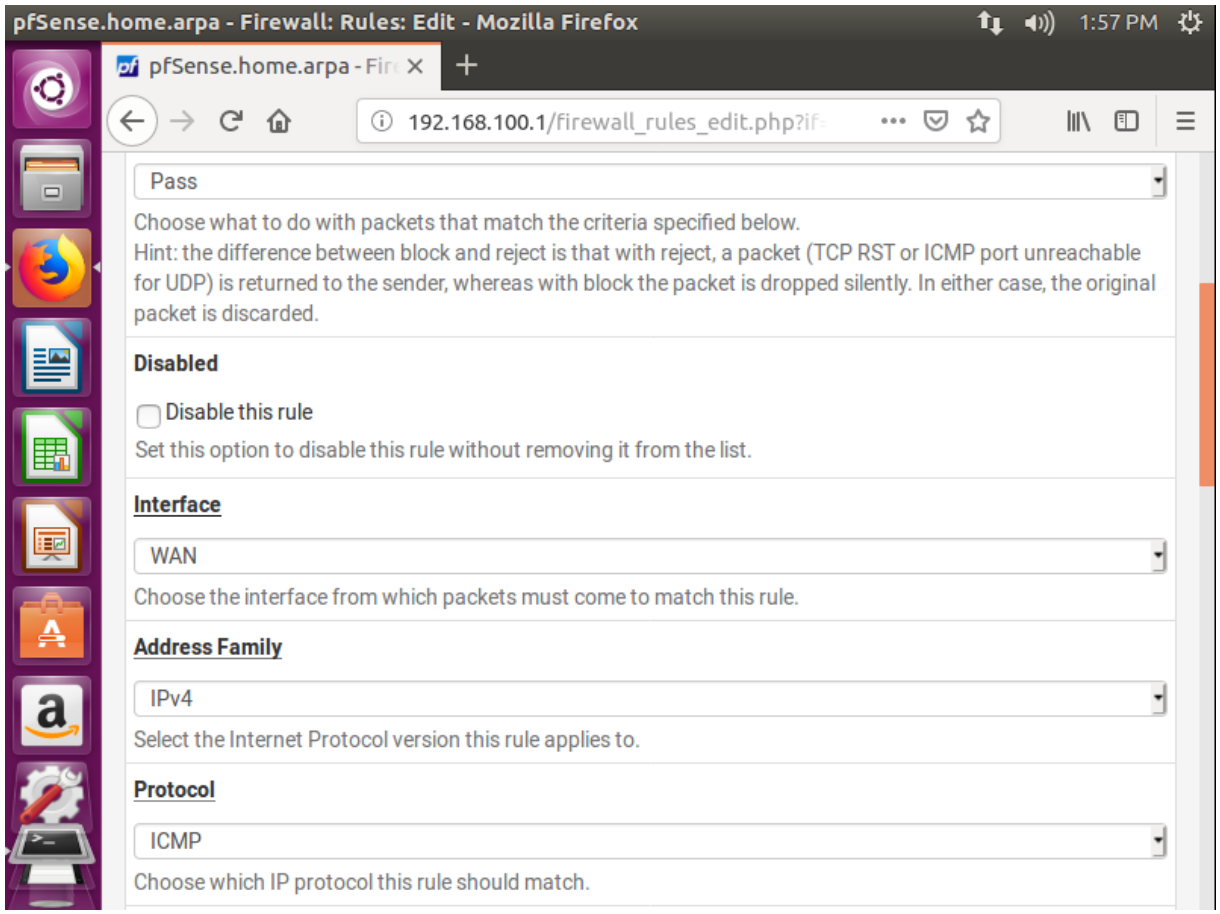
+ Máy Kali ping tới máy Windows Server External

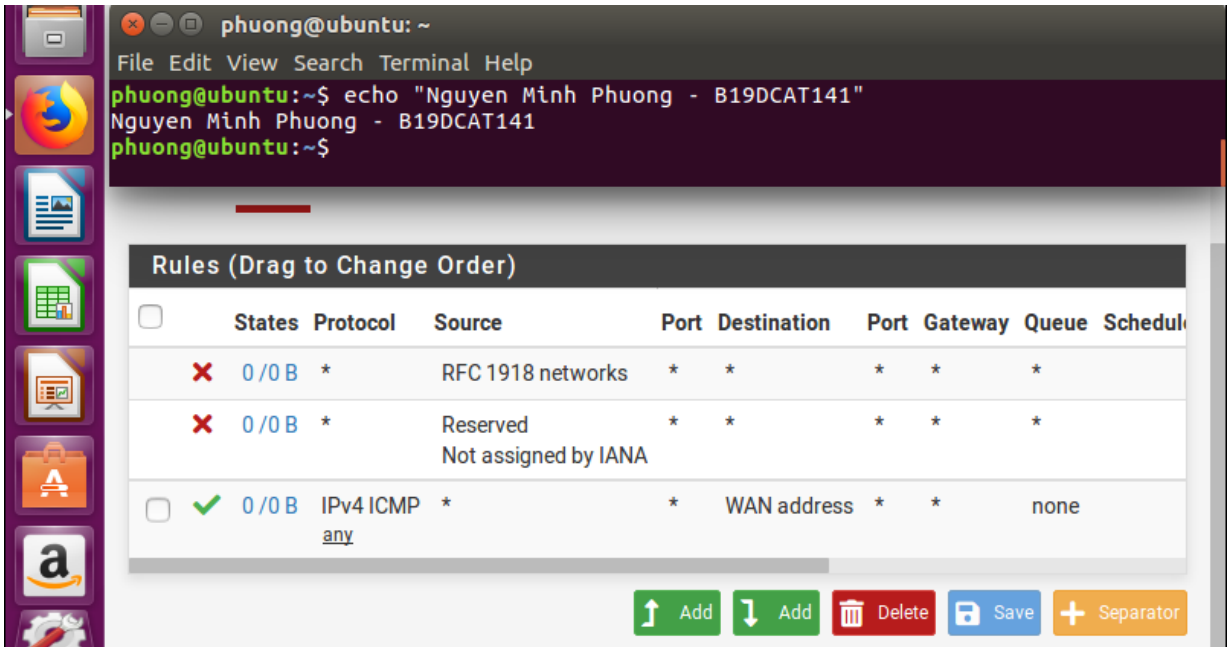
- Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

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



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

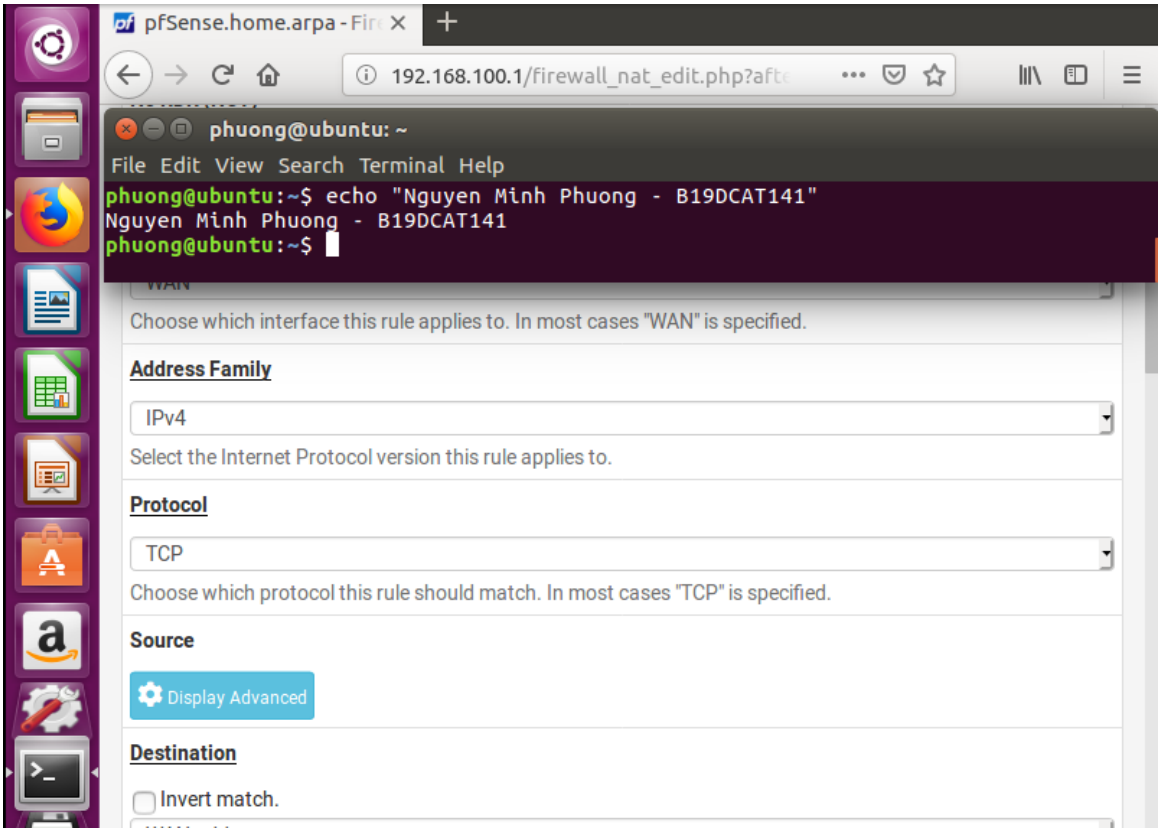

pfSense.home.arpa - Firewall: Rules: Edit - Mozilla Firefox
1:57 PM
pfSense.home.arpa - Fir
192.168.100.1/firewall_rules_edit.php?if
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP 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.

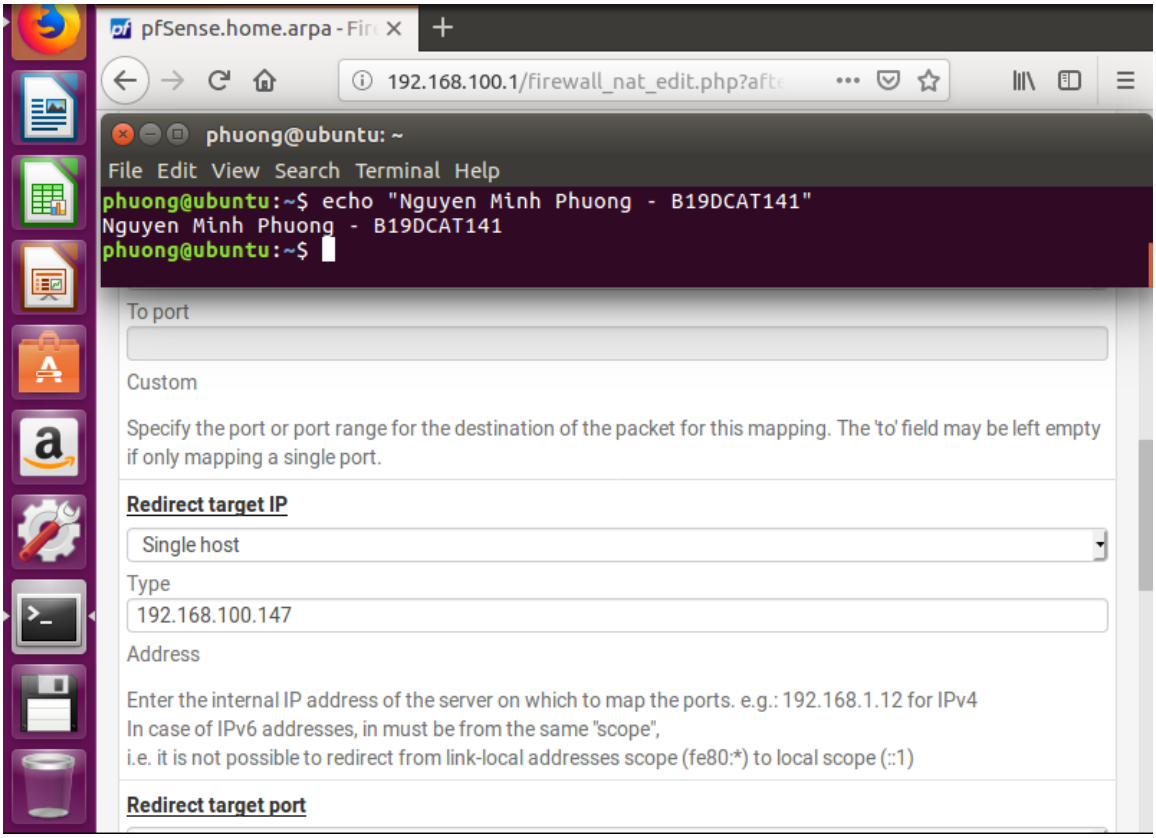

phuong@ubuntu: ~
File Edit View Search Terminal Help
phuong@ubuntu:~$ echo "Nguyen Minh Phuong - B19DCAT141"
Nguyen Minh Phuong - B19DCAT141
phuong@ubuntu:~$
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedul
0 /0 B * RFC 1918 networks * * * * *
0 /0 B * Reserved Not assigned by IANA * * * * *
0 /0 B IPv4 ICMP any * * WAN address * * none
Add
Add
Delete
Save
Separator

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

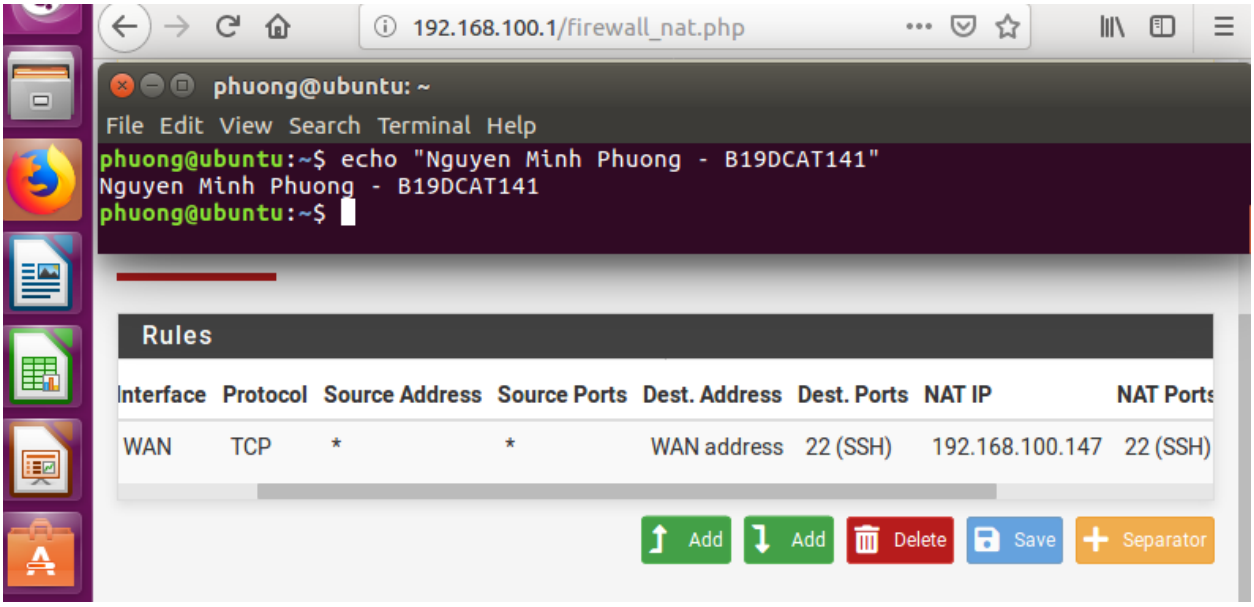
```
┌──(kali㉿b19dcat141-phuongnm-kali)-[~]
└─$ ping 10.10.19.1
PING 10.10.19.1 (10.10.19.1) 56(84) bytes of data.
64 bytes from 10.10.19.1: icmp_seq=1 ttl=128 time=0.513 ms
64 bytes from 10.10.19.1: icmp_seq=2 ttl=128 time=0.411 ms
64 bytes from 10.10.19.1: icmp_seq=3 ttl=128 time=0.330 ms
64 bytes from 10.10.19.1: icmp_seq=4 ttl=128 time=0.298 ms
64 bytes from 10.10.19.1: icmp_seq=5 ttl=128 time=0.453 ms
^C
--- 10.10.19.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4071ms
rtt min/avg/max/mdev = 0.298/0.401/0.513/0.078 ms
```

- 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.





+ 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.



+ Cài đặt và bật OpenSSH trên máy Ubuntu

```
root@ubuntu:/home/phuong-b19dcat141# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Thu 2022-04-07 07:45:19 PDT; 29s ago
 Main PID: 3024 (sshd)
   CGroup: /system.slice/ssh.service
           └─3024 /usr/sbin/sshd -D

Apr 07 07:45:19 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Apr 07 07:45:19 ubuntu sshd[3024]: Server listening on 0.0.0.0 port 22.
Apr 07 07:45:19 ubuntu sshd[3024]: Server listening on :: port 22.
Apr 07 07:45:19 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
Apr 07 07:45:44 ubuntu systemd[1]: Started OpenBSD Secure Shell server.

root@ubuntu:/home/phuong-b19dcat141# echo "Nguyen Minh Phuong_B19DCAT141"
Nguyen Minh Phuong_B19DCAT141
```

+ Trên máy Kali mạng External kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147hay không.

```
┌──(root💀b19dcat141-phuongnm-kali)-[/]
└─# ssh 10.10.19.1                                                    130 ×
root@10.10.19.1's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-30-generic x86_64)

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

107 updates can be applied immediately.
93 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

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


2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Mar 22 23:22:16 2022 from 10.10.19.148
root@B19DCAT205-Viet-Ubuntu:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.147  netmask 255.255.255.0  broadcast 192.168.100.255
        ether 00:0c:29:f7:d4:d3  txqueuelen 1000  (Ethernet)
        RX packets 7797  bytes 923255 (923.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1010  bytes 159293 (159.2 KB)
        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 44461  bytes 3254284 (3.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 44461  bytes 3254284 (3.2 MB)
```

```
┌──(root💀 b19dcat141-phuongnm-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
        ether 00:0c:29:ba:f7:b8  txqueuelen 1000  (Ethernet)
        RX packets 1643  bytes 168614 (164.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18455  bytes 1212971 (1.1 MiB)
        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 20  bytes 1000 (1000.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1000 (1000.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root💀 b19dcat141-phuongnm-kali)-[/]
└─# nmap 192.168.100.1
Starting Nmap 7.91 ( https://nmap.org ) at 2022-03-25 03:05 EDT
Nmap scan report for 192.168.100.1
Host is up (0.00048s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: 00:0C:29:2E:C3:15 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 18.21 seconds
```