

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



Môn: Thực tập cơ sở

BÀI BÁO THỰC TẬP CƠ SỞ
Bài 5: Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

Họ và tên giảng viên: PGS.TS.Đỗ Xuân Chợt
Họ và tên: Phạm Thanh Tùng
Mã sinh viên: B20DCAT171
Lớp: D20CQAT03-B
Số điện thoại: 0856915668

Hà Nội 2023

1. Tìm hiểu lý thuyết

1.1. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng VMware
VMware Workstation có nhiều tính năng của mạng giúp tạo và quản lý các mạng riêng tư, chia sẻ hoặc mạng cách ly bên trong VMware Workstation. Để bắt đầu cấu hình mạng trong VMware Workstation. Mở VMware Workstation > Chuyển đến Edit menu. Chọn Virtual Network Editor. Card mạng ảo trong VMware Workstation có các thao tác như: thêm, xóa một vmnet, sửa dải IP của một vmnet, cấu hình DHCP.

Có 3 mạng mặc định được tạo khi cài đặt VMware Workstation. Đó là vmnet0, vmnet1, vmnet8. Chúng là 3 chế độ khác nhau: Bridged, Host-only, NAT.

Bridged: Máy ảo hoạt động độc lập được kết nối với switch và router vật lý và trực tiếp nhận địa chỉ IP từ DHCP Server có mặt trong mạng lưới. Nó có quyền truy cập vào các máy khác trên mạng và có thể được các máy khác liên hệ trên mạng như thể là một máy tính vật lý.

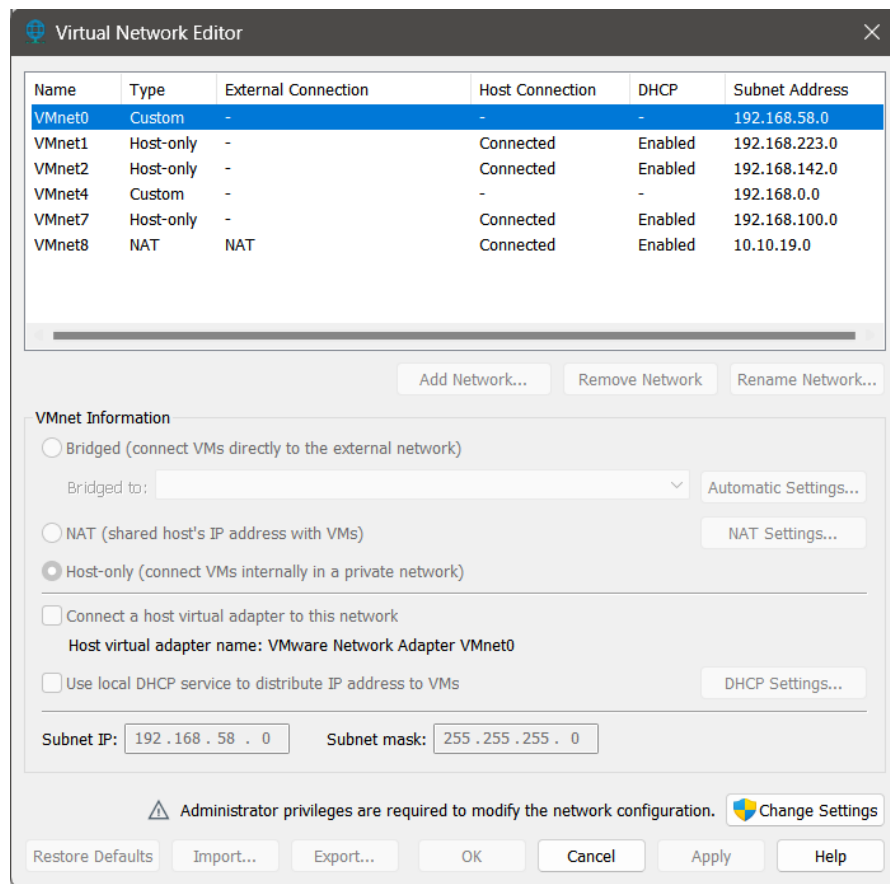
NAT: Đây là chế độ mạng mặc định được sử dụng và gán khi tạo một máy ảo. Ở chế độ này, máy ảo không có địa chỉ IP riêng trên mạng bên ngoài. Thay vào đó, một mạng riêng được thiết lập trên máy chủ lưu trữ. Máy ảo nhận một địa chỉ trên mạng đó từ máy chủ DHCP VMware ảo. Thiết bị VMware NAT truyền dữ liệu 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: Được sử dụng khi cần tạo một mạng hoàn toàn bị cô lập để máy ảo của bạn không thể thấy mạng khác hoặc Internet, cung cấp kết nối mạng giữa máy ảo và máy chủ, sử dụng bộ chuyển đổi Ethernet ảo hiển thị trên hệ điều hành máy chủ.

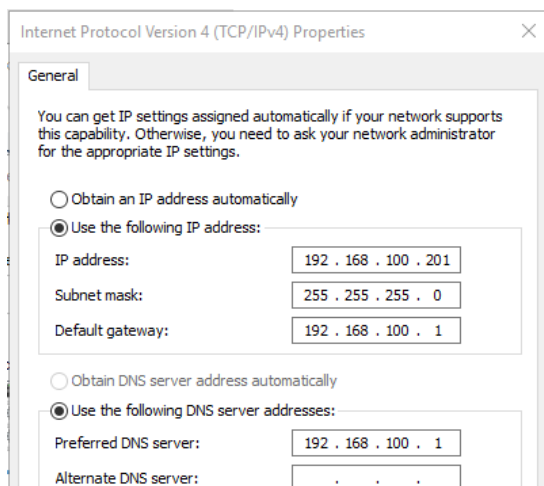
2. Nội dung thực hành

2.1. Cấu hình topo mạng

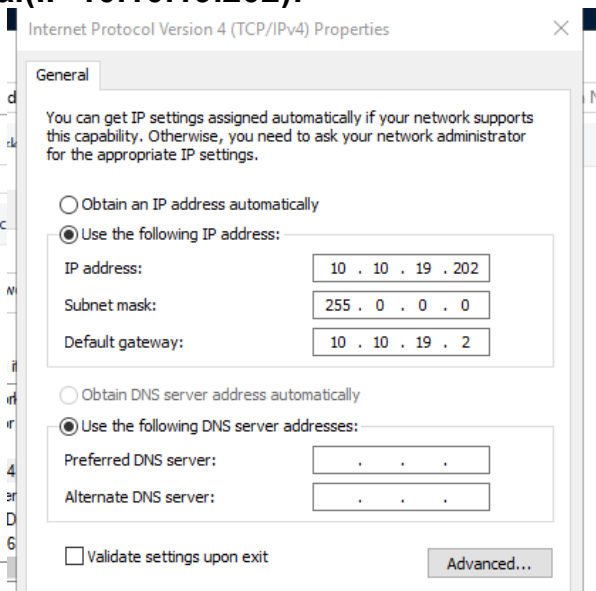
Tạo 2 subnet trên vmware, vmnet8 có địa chỉ 10.10.19.0/24 cho mạng Internal và vmnet7 có địa chỉ 192.168.100.0/24 cho mạng External:



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):

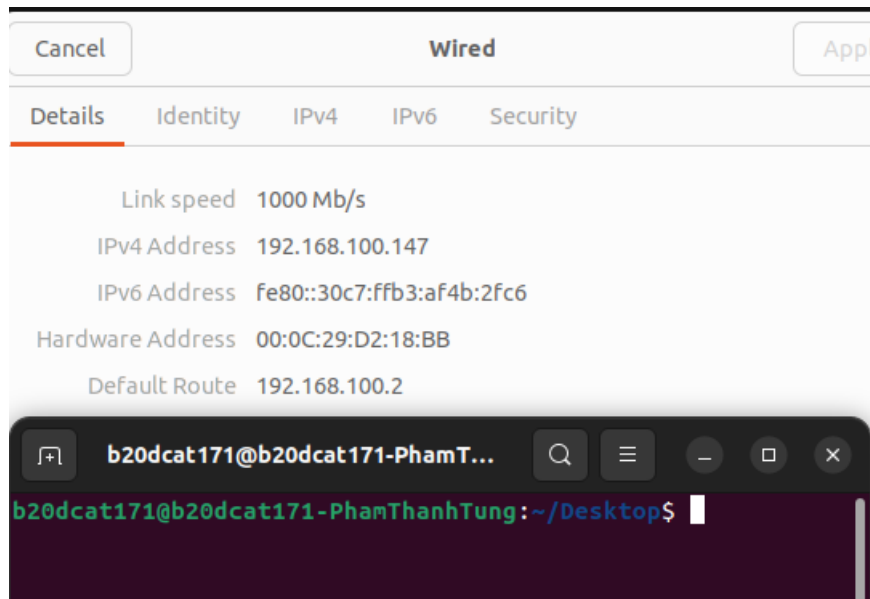


```
Administrator: C:\Windows\system32\cmd.exe - date
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>echo B20DCAT171 Pham Thanh Tung
B20DCAT171 Pham Thanh Tung
C:\Users\Administrator>date
The current date is: Thu 03/02/2023
Enter the new date: (mm-dd-yy)
```

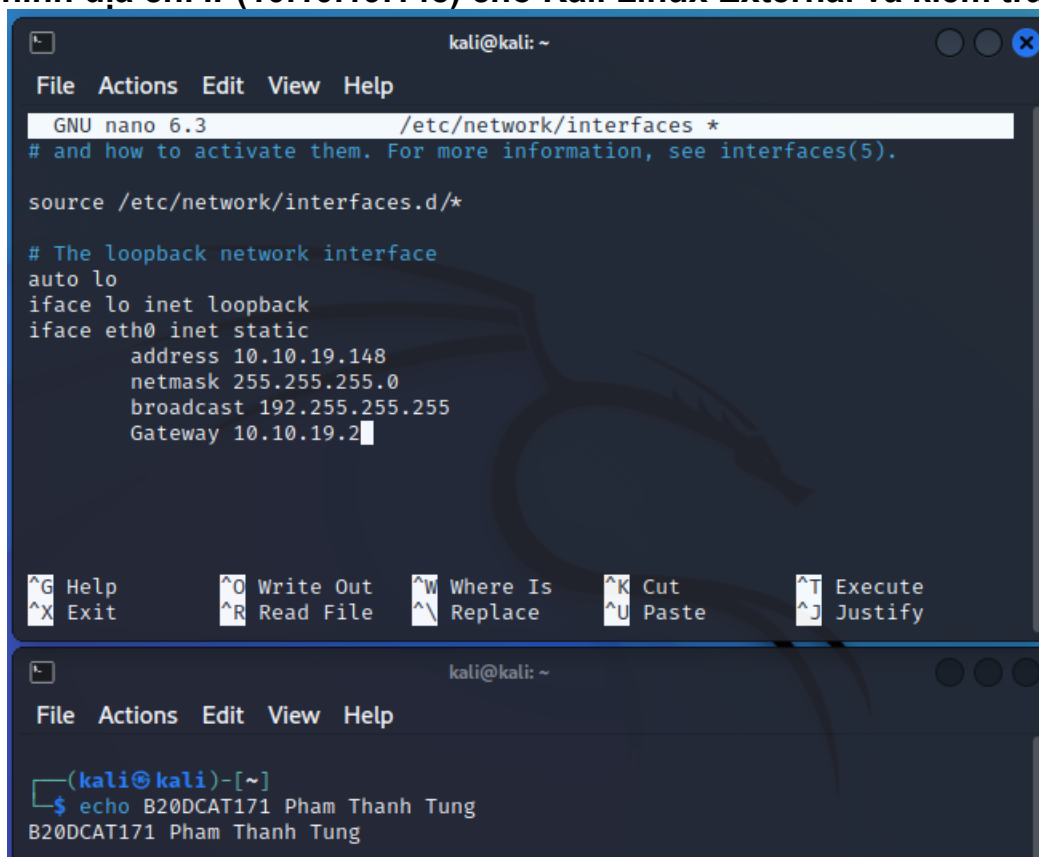


```
Administrator: C:\Windows\system32\cmd.exe - date
Pham Thanh Tung B20DCAT171
C:\Users\Administrator>date
The current date is: Thu 03/02/2023
Enter the new date: (mm-dd-yy)
```

Cấu hình địa chỉ IP(192.168.100.147) cho Ubuntu Linux Internal và kiểm tra:



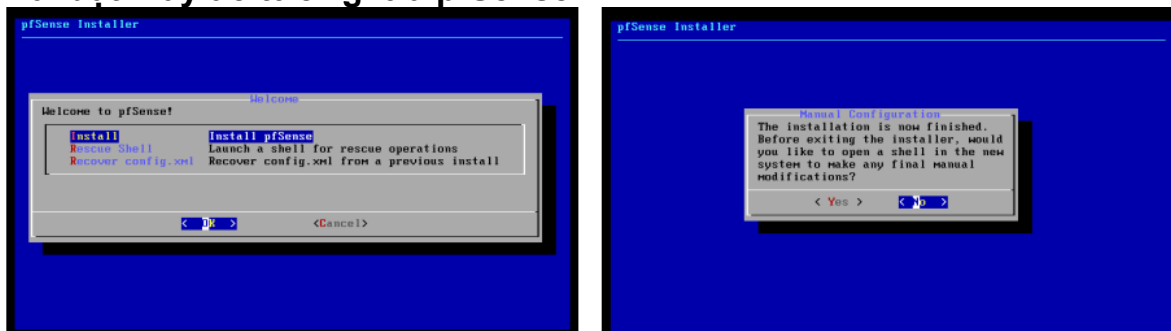
Cấu hình địa chỉ IP(10.10.19.148) cho Kali Linux External và kiểm tra:



Cấu hình địa chỉ IP(192.168.100.3) cho Kali Linux Internal và kiểm tra:

```
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
(kali@B20DCAT171-Tung-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  
        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:29:4b:50:b8 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.100.3/24 brd 192.168.100.255 scope global eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::20c:29ff:fe4b:50b8/64 scope link  
        valid_lft forever preferred_lft forever  
  
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo B20DCAT171 Pham Thanh Tung  
B20DCAT171 Pham Thanh Tung  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ date  
Thu Mar  2 01:13:04 AM EST 2023  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$
```

Cài đặt máy ảo tường lửa pfSense:



Cấu hình 2 interface cho pfSense; em0 có IP 10.10.19.1 cho mạng EXTERNAL, em1 có IP 192.168.100.1 cho mạng INTERNAL:

```

Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 81ceb37283f62900f21a

*** 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) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █

```

Thử nghiệm ping các máy trong mạng với PfSense: ping Windows Server 2003 Internal và External:

```

[2.6.0-RELEASE][root@pfSense.home.arp]/root: ping -c 1 192.168.100.201
PING 192.168.100.201 (192.168.100.201): 56 data bytes
64 bytes from 192.168.100.201: icmp_seq=0 ttl=128 time=1.403 ms

--- 192.168.100.201 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.403/1.403/1.403/0.000 ms
[2.6.0-RELEASE][root@pfSense.home.arp]/root: ping -c 1 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=0.616 ms

--- 10.10.19.202 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.616/0.616/0.616/0.000 ms

```

ping Kali Linux Internal và External:

```

[2.6.0-RELEASE][root@pfSense.home.arp]/root: ping -c 1 192.168.100.3
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=0.906 ms

--- 192.168.100.3 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.906/0.906/0.906/0.000 ms
[2.6.0-RELEASE][root@pfSense.home.arp]/root: ping -c 1 10.10.19.148
PING 10.10.19.148 (10.10.19.148): 56 data bytes
64 bytes from 10.10.19.148: icmp_seq=0 ttl=64 time=0.639 ms

--- 10.10.19.148 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.639/0.639/0.639/0.000 ms

```

ping Ubuntu Internal:

```

Enter an option: 7

Enter a host name or IP address: 192.168.100.147

PING 192.168.100.147 (192.168.100.147): 56 data bytes
64 bytes from 192.168.100.147: icmp_seq=0 ttl=64 time=0.927 ms
64 bytes from 192.168.100.147: icmp_seq=1 ttl=64 time=1.216 ms
64 bytes from 192.168.100.147: icmp_seq=2 ttl=64 time=1.199 ms

--- 192.168.100.147 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.927/1.114/1.216/0.132 ms

```

Thử nghiệm ping các máy Kali linux và Ubuntu trong mạng Internal bằng Windows Server Internal:

```

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=7ms TTL=64
Reply from 192.168.100.147: bytes=32 time=10ms 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 = 1ms, Maximum = 10ms, Average = 4ms

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=11ms TTL=64
Reply from 192.168.100.3: bytes=32 time=1ms TTL=64
Reply from 192.168.100.3: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 3ms

C:\Users\Administrator>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Administrator>date
The current date is: Thu 03/02/2023
Enter the new date: (mm-dd-yy)

```

Thử nghiệm ping các máy Windows Server và Ubuntu trong mạng Internal bằng Kali Linux Internal:

```
File Actions Edit View Help
(kali@B20DCAT171-Tung-Kali)-[~]
$ ping -c 1 192.168.100.147
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=1.12 ms

— 192.168.100.147 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.117/1.117/1.117/0.000 ms

(kali@B20DCAT171-Tung-Kali)-[~]
$ ping -c 1 192.168.100.201
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=0.828 ms

— 192.168.100.201 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.828/0.828/0.828/0.000 ms

kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help
(kali@B20DCAT171-Tung-Kali)-[~]
$ echo B20DCAT171 Pham Thanh Tung
B20DCAT171 Pham Thanh Tung

(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Thu Mar  2 02:43:36 AM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

Thử nghiệm ping các máy Windows Server và Kali Linux trong mạng Internal bằng Ubuntu Internal:


```
b20dcat171@b20dcat171-PhamThanhTung: ~/Desktop
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$ ping -c 1 192.168.100.3
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=0.316 ms

--- 192.168.100.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.316/0.316/0.316/0.000 ms
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$ ping -c 1 192.168.100.201
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=11.5 ms

--- 192.168.100.201 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.547/11.547/11.547/0.000 ms
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$

b20dcat171@b20dcat171-PhamThanhTung: ~/Desktop
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$ echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$ date
Thứ năm, 02 Tháng 3 năm 2023 14:44:45 +07
b20dcat171@b20dcat171-PhamThanhTung:~/Desktop$
```

Thử nghiệm ping lẫn nhau 2 máy Windows Server và Kali Linux trong mạng External:

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
$ ping -c 1 10.10.19.202
PING 10.10.19.202 (10.10.19.202) 56(84) bytes of data.
64 bytes from 10.10.19.202: icmp_seq=1 ttl=128 time=0.389 ms

--- 10.10.19.202 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.389/0.389/0.389/0.000 ms

(kali@B20DCAT171-Tung-Kali)-[~]
$

kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
$ echo B20DCAT171 Pham Thanh Tung
B20DCAT171 Pham Thanh Tung

(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Thu Mar  2 02:47:36 AM EST 2023

(kali@B20DCAT171-Tung-Kali)-[~]
$
```

```

C:\Users\Administrator>ping -n 1 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

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

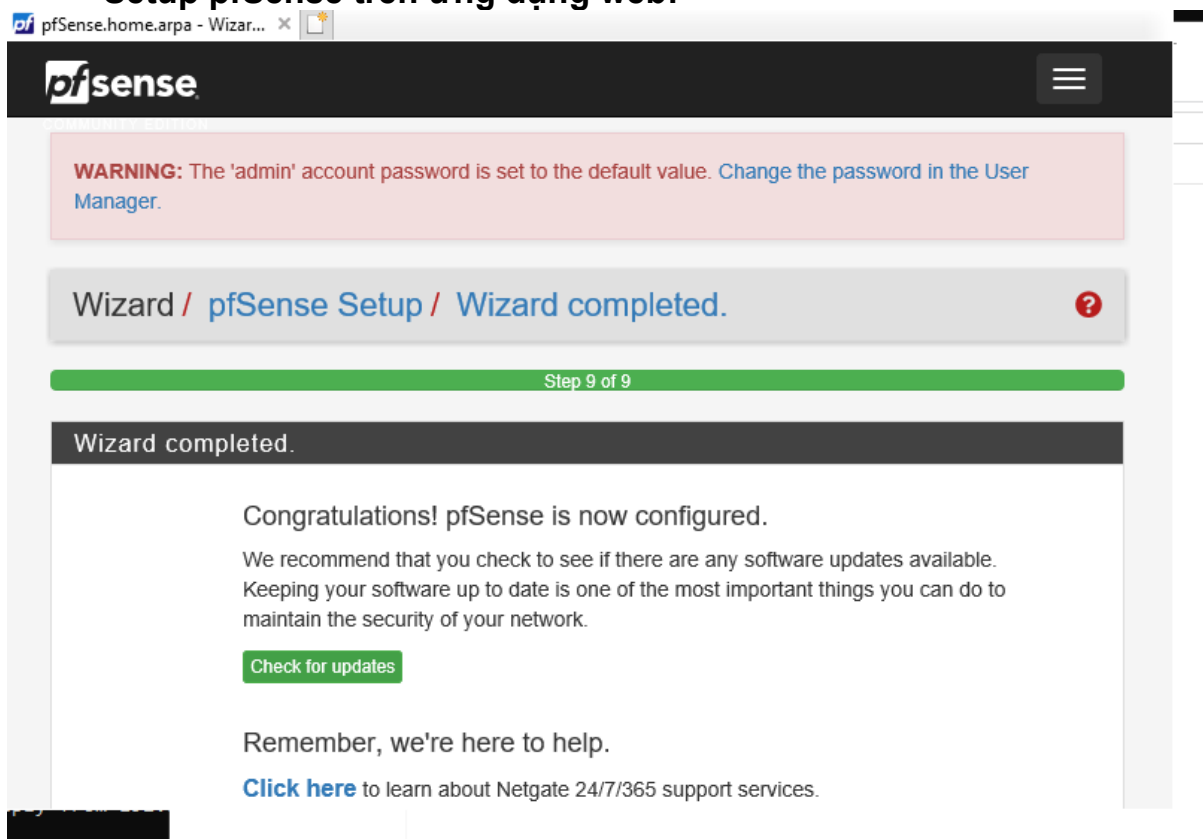
C:\Users\Administrator>echo Pham Thanh Tung B20DCAT171
Pham Thanh Tung B20DCAT171

C:\Users\Administrator>date
The current date is: Thu 03/02/2023
Enter the new date: (mm-dd-yy)

```

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

Setup pfSense trên ứng dụng web:



The screenshot shows the pfSense web interface at the URL `pfSense.home.arpa`. The page features a dark header with the pfSense logo and a hamburger menu. A red warning box at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, a breadcrumb trail reads "Wizard / pfSense Setup / Wizard completed." with a red question mark icon. A green progress bar indicates "Step 9 of 9". The main content area has a dark header "Wizard completed." and a white body with the text: "Congratulations! pfSense is now configured. We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network." A green button labeled "Check for updates" is present. At the bottom, it says "Remember, we're here to help." and provides a link: "Click here to learn about Netgate 24/7/365 support services."

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

pfSense System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit

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 LAN ▾
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 any ▾ Destination Address / ▾

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:

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

Interface LAN
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 any Destination Address /

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description B20DCAT171 Pham Thanh Tung
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options Display Advanced

Save

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

```
kali@B20DCAT171-Tung-Kali: ~
File Actions Edit View Help

(kali@B20DCAT171-Tung-Kali)-[~]
$ ping -c 1 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=0.450 ms

— 10.10.19.1 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.450/0.450/0.450/0.000 ms

(kali@B20DCAT171-Tung-Kali)-[~]
$ echo B20DCAT171 Pham Thanh Tung
B20DCAT171 Pham Thanh Tung

(kali@B20DCAT171-Tung-Kali)-[~]
$ date
Fri Mar 3 03:31:39 AM EST 2023
```

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.)

Source	Display Advanced		
Destination	<input type="checkbox"/> Invert match.	WAN address	
	Type	Address/mask	
Destination port range	SSH	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	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.			
Description	Cauhinh Nat-SSH B20DCAT171		
A description may be entered here for administrative reference (not parsed).			
No XMLRPC Sync	<input type="checkbox"/> 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	Rule NAT Cauhinh Nat-SSH		
View the filter rule			
Rule Information			

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

```
b20dcat171@b20dcat171: ~  
File Actions Edit View Help  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ ssh b20dcat171@10.10.19.1  
b20dcat171@10.10.19.1's password:  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-43-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
269 updates can be applied immediately.  
119 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 proxy settings  
  
Last login: Fri Mar 3 18:04:30 2023 from 10.10.19.148  
b20dcat171@b20dcat171:~$ 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  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 00:0c:29:35:3d:e3 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.100.147/24 brd 192.168.100.255 scope global noprefixroute ens33  
        valid_lft forever preferred_lft forever  
    inet6 fe80::17f1:4f0e:163f:90/64 scope link noprefixroute  
  
kali@B20DCAT171-Tung-Kali: ~  
File Actions Edit View Help  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ echo B20DCAT171 Pham Thanh Tung  
B20DCAT171 Pham Thanh Tung  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$ date  
Fri Mar 3 06:06:13 AM EST 2023  
  
(kali@B20DCAT171-Tung-Kali)-[~]  
$
```