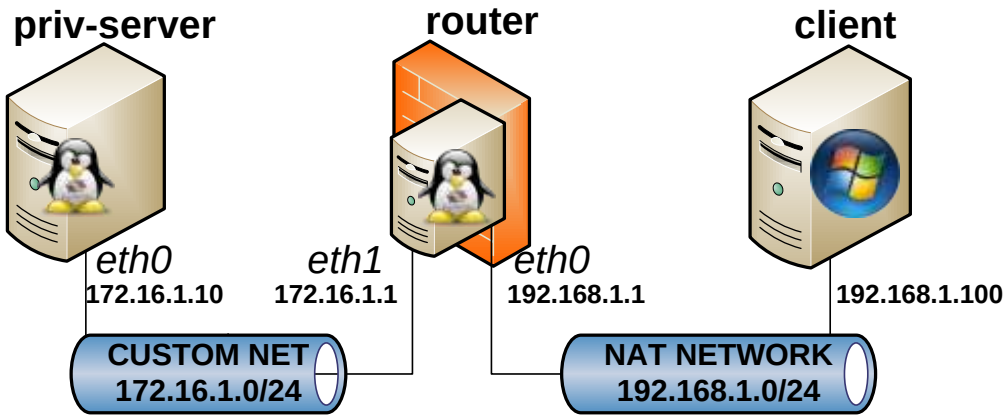
Bài thực hành

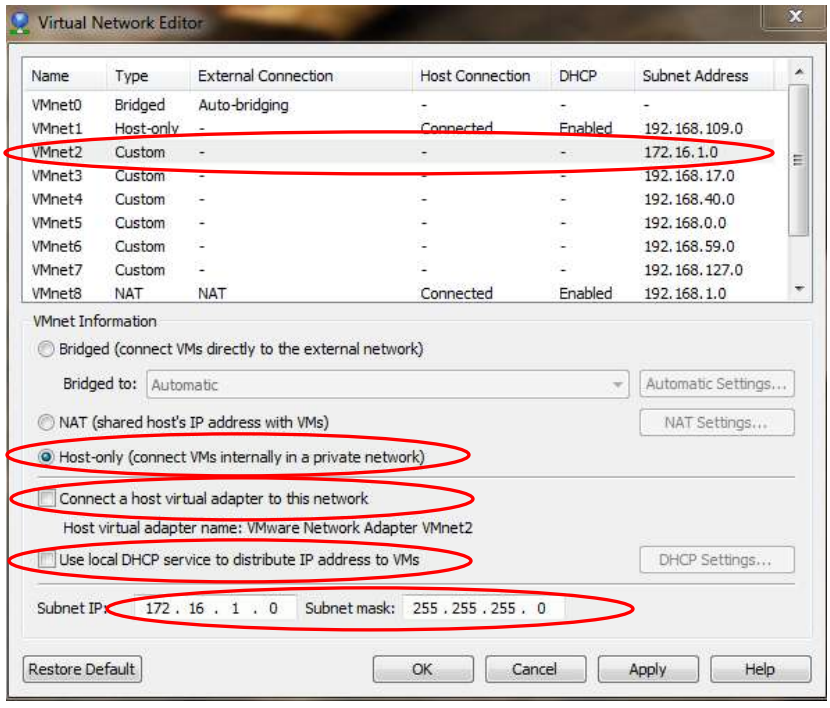
Cài đặt và cấu hình Router/DHCP Server/Firewall

I. Mô hình hệ thống

Trong bài thực hành này, bạn cần sử dụng 02 máy ảo Linux và máy thật Windows kết nối theo mô hình bên dưới



Để tạo mạng Custom Network như yêu cầu bài thực hành, bạn mở VMware Virtual Network Editor và chỉnh sửa VMnet2 như hình bên dưới.



Cần chú ý **<u>bỏ</u>** các lựa chọn "*Connect a host virtual adapter to this network*" và "*Use local DHCP service to distribute IP address to VMs*"

II. Cài đặt và cấu hình dịch vụ DHCP

Cài đặt và cấu hình DHCP Server trên máy ảo Linux làm Router

Bước 1. Cấu hình card mạng cho máy ảo Linux làm ***Router*** và làm ***Private Server*** với địa chỉ như trong sơ đồ kết nối ở trên. Tắt firewall trên các máy ảo Linux.

```
[root@router]# ifconfig eth0 192.168.1.1/24 up
[root@router]# ifconfig eth1 172.16.1.1/24 up
[root@router]# service iptables stop
```

```
[root@priv-server]# ifconfig eth0 172.16.1.10/24 up
[root@priv-server]# service iptables stop
```

Bước 2. Kiểm tra lại để đảm bảo:

- Máy ảo Private Server chỉ có thể ping đến máy ảo Router
- Máy thật Windows chỉ có thể ping đến máy ảo Router
- Máy ảo Router có thể ping đến cả Private Server và máy Windows

Bước 3. [Trên máy ảo ***Router***] Kiểm tra package **dhcp** đã được cài đặt hay chưa. Nếu chưa cần tiến hành cài đặt package này qua **yum** hoặc **rpm**

```
[root@router]# rpm -qa | grep dhcp
dhcpv6-client-1.0.10-18.el5
[root@router]# yum install dhcp
[root@router]# rpm -qa | grep dhcp
dhcp-3.0.5-23.el5
dhcpv6-client-1.0.10-18.el5
```

Bước 4. [Trên máy ảo ***Router***] Mở file ***/etc/dhcpd.conf*** để xem hướng dẫn copy file cấu hình mẫu cho dịch vụ dhcpd từ ***/usr/share/doc/dhcp-3.0.5***. Copy file mẫu này và xem các thông tin cấu hình chính

```
[root@router]# cat /etc/dhcpd.conf
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
[root@router]# cd /usr/share/doc/dhcp-3.0.5/
[root@router]# cp ./dhcpd.conf.sample /etc/dhcpd.conf
cp: overwrite `/etc/dhcpd.conf'? y
[root@router]# cat /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;        #không cập nhật động DNS

#Thông tin về subnet và netmask sẽ được cấp phát cho client
subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
…
```

```
        #Dải IP sẽ được cấp phát cho client
        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600; #Thời gian mặc định cấp IP cho client
        max-lease-time 43200;     #Thời gian tối đa cấp IP cho client

        #Danh sách các host luôn được cấp một IP cố định dựa trên MAC
        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
```

Bước 5. [Trên máy ảo ***Router***] Chỉnh sửa lại file cấu hình để thể hiện đúng sơ đồ hệ thống như trong bài thực hành này

```
[root@router]# vi /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;

#Chỉnh lại subnet và netmask về dải 172.16.1.0/24
subnet 172.16.1.0 netmask 255.255.255.0 {

# --- default gateway
        #Chỉnh lại gateway trỏ về router (172.16.1.1)
        option routers                  172.16.1.1;
        option subnet-mask              255.255.255.0;

        #Chỉnh lại domain thành internal.ipmac.lab, DNS trỏ về router
        option nis-domain               "internal.ipmac.lab";
        option domain-name              "internal.ipmac.lab";
        option domain-name-servers      172.16.1.1;

        option time-offset              -18000; # Eastern Standard Time
…

        #Cấp phát IP cho các client 172.16.1.100 đến 172.16.1.200
        range dynamic-bootp 172.16.1.100 172.16.1.200;
        default-lease-time 21600; #Thời gian mặc định cấp IP cho client
        max-lease-time 43200;     #Thời gian tối đa cấp IP cho client

        # we want the nameserver to appear at a fixed address
        #host ns {
        #         next-server marvin.redhat.com;
        #         hardware ethernet 12:34:56:78:AB:CD;
        #         fixed-address 207.175.42.254;
        #}
}
```

Bước 6. [Trên máy ảo ***Router***] Khởi động dịch vụ **dhcpd** và theo dõi tình hình cấp phát DHCP

```
[root@router]# service dhcpd start
Starting dhcpd:                                            [  OK  ]
[root@router]# tail -f /var/lib/dhcpd/dhcpd.leases
```

Cài đặt và cấu hình DHCP Client trên máy ảo Linux làm Private Server

Bước 7. [Trên máy ảo ***Private Server***] Kiểm tra lại file cấu hình card mạng *eth0* để đảm bảo đang ở chế độ nhận IP qua DHCP

```
[root@priv-server]# vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
HWADDR=00:0C:29:E3:35:81
TYPE=Ethernet
USERCTL=no
IPV6INIT=no
```

Bước 8. [Trên máy ảo ***Private Server***] Khởi động lại dịch vụ network, sau đó kiểm tra lại địa chỉ IP của *eth0* để thấy lúc này *eth0* đã nhận địa chỉ được cấp bởi DHCP Server (trong khoảng 172.16.1.100 đến 172.16.1.200). Kiểm tra bảng route để thấy địa chỉ Gateway đã được đặt.

```
[root@priv-server]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0… done.:
                                                           [  OK  ]
[root@priv-server]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E3:35:81
          inet addr:172.16.1.200  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::213:d4ff:fee3:3581/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:140 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13331 (13.0 KiB)  TX bytes:7314 (7.1 KiB)
[root@priv-server]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.1.0      0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
0.0.0.0         172.16.1.1      0.0.0.0         UG        0 0          0 eth0
```

Bước 9. [Trên máy ảo ***Router***] Kiểm tra tình trạng cấp phát DHCP

```
[root@router]# tail -f /var/lib/dhcpd/dhcpd.leases
…
lease 172.16.1.200 {
       starts 1 2011/03/10 22:13:33;
       ends 2 2011/03/11 04:13:33;
       binding state active;
       next binding state free;
       hardware ethernet 00:0c:29:e3:35:81;
}
```

(Tùy chọn) Cấu hình DHCP Server để cấp phát cố định địa chỉ IP cho client

Bước 10. [Trên máy ảo ***Private Server***] Lấy thông tin về địa chỉ MAC của *eth0*

```
[root@priv-server]# ifconfig eth0 | grep HWaddr
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E3:35:81
```

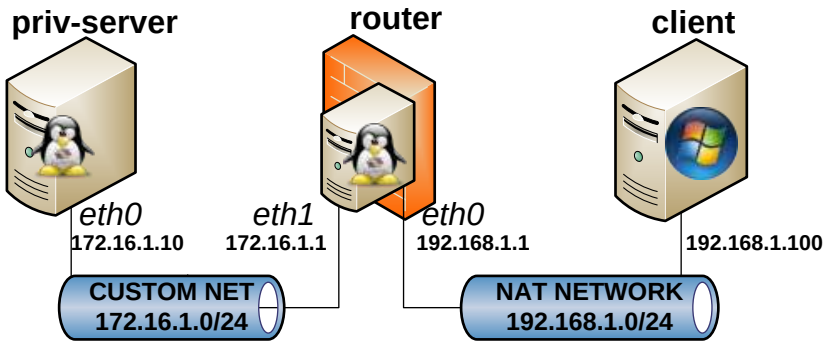
Bước 11. [Trên máy ảo ***Router***] Cấu hình lại dịch vụ DHCP để cấp phát cố định địa chỉ 172.16.1.10 cho ***Private Server*** dựa trên thông tin về địa chỉ MAC vừa có được ở bước trên. Khởi động lại dịch vụ DHCP sau khi hoàn tất.

```
[root@router]# vi /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
…
        # we want the nameserver to appear at a fixed address
        #host ns {
        #        next-server marvin.redhat.com;
        #        hardware ethernet 12:34:56:78:AB:CD;
        #        fixed-address 207.175.42.254;
        #}

        host priv-server {
                hardware ethernet 00:0C:29:E3:35:81;
                fixed-address 172.16.1.10;
                option host-name "priv-server";
        }
}
[root@router]# service dhcpd restart
```

Bước 12. [Trên máy ảo ***Private Server***] Khởi động lại dịch vụ network, sau đó kiểm tra lại địa chỉ IP của *eth0* để thấy lúc này *eth0* đã nhận địa chỉ được cấp bởi DHCP Server là 172.16.1.10

```
[root@priv-server]# service network restart
Shutting down interface eth0:                              [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:
Determining IP information for eth0… done.:
                                                           [  OK  ]
[root@priv-server]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:E3:35:81
          inet addr:172.16.1.10  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::213:d4ff:fee3:3581/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:140 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13331 (13.0 KiB)  TX bytes:7314 (7.1 KiB)
```

III. Cấu hình Firewall/NAT trên Router với iptables



Trong bài thực hành này chúng ta sẽ cấu hình ***iptables*** trên ***Router*** để chỉ cho phép các kết nối sau:

Kết nối đến / Kết nối từ	Private Server	Router	Windows Client
Private Server	n/a	DNS, SSH, PING	ALL
Router	SSH	n/a	DNS, SSH, PING
Windows Client	SSH, HTTP	SSH	n/a

Cài đặt và khởi tạo iptables trên máy ảo làm Router

Bước 1. Cấu hình card mạng cho máy ảo Linux làm ***Router*** và làm ***Private Server*** với địa chỉ như trong sơ đồ kết nối ở trên. Tắt ***iptables*** trên máy ***Private Server***

```
[root@router]# ifconfig eth0 192.168.1.1/24 up
[root@router]# ifconfig eth1 172.16.1.1/24 up
```

```
[root@priv-server]# ifconfig eth0 172.16.1.10/24 up
[root@priv-server]# service iptables stop
```

Bước 2. Kiểm tra lại để đảm bảo:

- Máy ảo Private Server chỉ có thể ping đến máy ảo Router
- Máy thật Windows chỉ có thể ping đến máy ảo Router
- Máy ảo Router có thể ping đến cả Private Server và máy Windows

Bước 3. [Trên máy ảo ***Router***] Kiểm tra package ***iptables*** đã được cài đặt hay chưa. Nếu chưa cần tiến hành cài đặt package này qua **yum** hoặc **rpm**

```
[root@router]# rpm -qa | grep iptables
iptables-1.3.5-5.3.el5_4.1
iptables-ipv6-1.3.5-5.3.el5_4.1
```

Bước 4. [Trên máy ảo ***Router***] Xem file cấu hình của ***iptables*** trong ***/etc/sysconfig***

```
[root@router]# cat /etc/sysconfig/iptables-config
#Các module sẽ được load cùng iptables
IPTABLES_MODULES="ip_conntrack_netbios_ns ip_conntrack_ftp"

#Có unload các module khi restart/stop dịch vụ hay không
IPTABLES_MODULES_UNLOAD="yes"
```

```
#Có lưu các rule của firewall vào /etc/sysconfig/iptables khi stop dịch vụ hay
#không
IPTABLES_SAVE_ON_STOP="no"

#Có lưu các rule của firewall vào /etc/sysconfig/iptables khi restart dịch vụ
#hay không
IPTABLES_SAVE_ON_RESTART="no"

#Có lưu lại các counter vào /etc/sysconfig/iptables khi stop hay restart dịch
#vụ hay không
IPTABLES_SAVE_COUNTER="no"

# Có hiển thị địa chỉ IP và port ở dạng số trong status output hay không
IPTABLES_STATUS_NUMERIC="yes"

# Có hiển thị status output ở dạng verbose hay không
IPTABLES_STATUS_VERBOSE="no"

# Có đánh số thứ tự các dòng status output hay không
IPTABLES_STATUS_LINENUMBERS="yes"
```

Bước 5. [Trên máy ảo ***Router***] Khởi động dịch vụ ***iptables*** và xem các rule hiện có

```
[root@router]# service iptables start
Flushing firewall rules:                                   [  OK  ]
Setting chains to policy ACCEPT: nat mangle filter         [  OK  ]
Unloading iptables modules:                                [  OK  ]
Applying iptables firewall rules:                          [  OK  ]
Loading additional iptables modules: ip_conntrack_netbios_n [  OK  ]
[root@router]# iptales -L -t filter
[root@router]# iptales -L -t nat
[root@router]# iptales -L -t mangle
```

Bước 6. [Trên máy ảo ***Router***] Lưu lại các rule hiện có ra file và hủy tất cả các rule trên ***iptables***

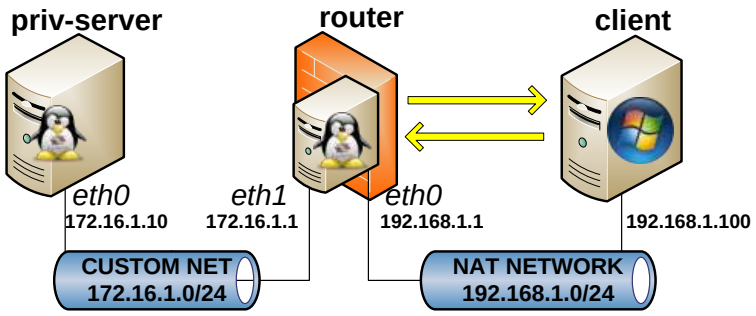
```
[root@router]# iptables-save > /tmp/iptables.rules
[root@router]# cat /tmp/iptables.rules
[root@router]# iptales -F -t filter
[root@router]# iptales -F -t nat
[root@router]# iptales -F -t mangle
```

Bước 7. [Trên máy ảo ***Router***] Cấu hình chính sách để Router không nhận (DROP) tất cả các gói tin trên mọi chain

```
[root@router]# iptables -P INPUT DROP
[root@router]# iptables -P FORWARD DROP
[root@router]# iptables -P OUTPUT DROP
[root@router]# iptables -L
```

Bước 8. Kiểm tra để đảm bảo các máy ảo ***Private Server*** và máy thật Windows đều không thể ping được đến Router cũng như ngược lại.

Cấu hình iptables cho phép các kết nối từ Router đến Client và ngược lại



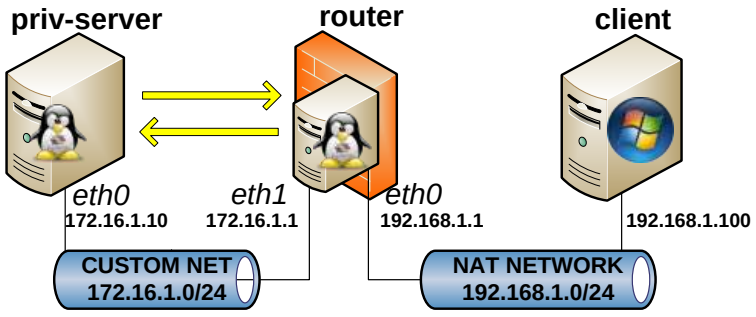
Bước 9. [Trên máy ảo ***Router***] Cấu hình cho phép các kết nối dịch vụ DNS, SSH, và PING từ ***Router*** ra bên ngoài

```
[root@router]# iptables -t filter -A OUTPUT -o eth0 -p udp  --destination-port
53 -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A OUTPUT -o eth0 -p tcp  --destination-port
ssh -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A OUTPUT -o eth0 -p icmp --icmp-type ping
-m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A INPUT -i eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Bước 10. [Trên máy ảo ***Router***] Cấu hình cho phép các kết từ bên ngoài đến dịch vụ SSH trên Router

```
[root@router]# iptables -t filter -A INPUT  -i eth0 -p tcp --destination-port
ssh -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A OUTPUT -o eth0 -p tcp --destination-port
ssh -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Cấu hình iptables cho phép kết nối từ Router đến Private Server và ngược lại



Bước 11. [Trên máy ảo ***Router***] Cấu hình cho phép các kết nối từ Router đến dịch vụ SSH trên Private Server

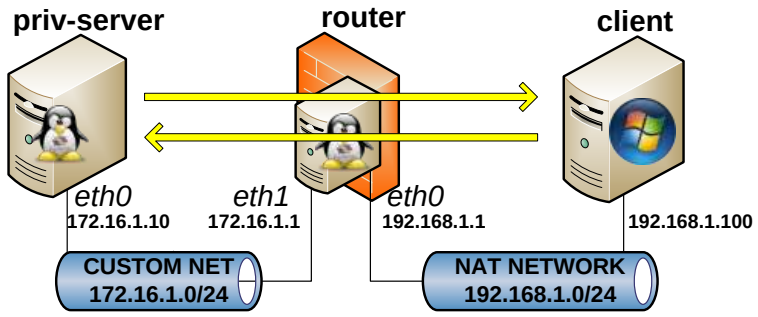
```
[root@router]# iptables -t filter -A OUTPUT -o eth1 -p tcp --destination-port
ssh -m state --state NEW -j ACCEPT
```

```
[root@router]# iptables -t filter -A INPUT -i eth1 -p tcp --destination-port
ssh -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Bước 12. [Trên máy ảo ***Router***] Cấu hình cho phép Private Server kết nối đến dịch vụ DNS, SSH và PING trên Router

```
[root@router]# iptables -t filter -A INPUT -i eth1 -p udp  --destination-port
53 -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A INPUT -i eth1 -p tcp  --destination-port
ssh -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A INPUT -i eth1 -p icmp --icmp-type ping
-m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A OUTPUT -o eth1 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Cấu hình NAT cho phép máy ảo Private Server kết nối ra bên ngoài



Bước 13. [Trên máy ảo ***Router***] Kiểm tra đảm bảo module ***iptable_nat*** đã được load trong kernel

```
[root@router]# lsmod | grep iptable_nat
iptable_nat            11077  0
```

Bước 14. [Trên máy ảo ***Router***] Cấu hình cho phép IP Forwarding giữa các card mạng. Chỉnh sửa file ***/etc/sysctl.conf*** để thay đổi có hiệu lực kể cả sau khi reboot hệ thống.

```
[root@router]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@router]# vi /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Bước 15. [Trên máy ảo ***Router***] Cấu hình NAT (Masquerade) trên ***iptables*** cho phép các kết nối từ Private Server ra bên ngoài

```
[root@router]# iptables –A POSTROUTING –t nat –o eth0 –s 172.16.1.0/24 –d 0/0
–j MASQUERADE
```

Bước 16. [Trên máy ảo ***Router***] Cấu hình cho phép mọi các kết nối từ Private Server ra bên ngoài

```
[root@router]# iptables -t filter -A FORWARD -i eth1 -o eth0 -m state --state
NEW -j ACCEPT

[root@router]# iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Bước 17. [Trên máy ảo ***Router***] Cấu hình chỉ cho phép từ bên ngoài kết nối đến các dịch vụ Web và dịch vụ SSH trên ***Private Server***

```
[root@router]# iptables -t nat -A PREROUTING -i eth0 -p tcp --destination-port
80 -j DNAT --to-destination 172.16.1.10:80

[root@router]# iptables -t filter -A FORWARD -i eth0 -p tcp --destination-port
80 -m state --state NEW -j ACCEPT

[root@router]# iptables -t nat -A PREROUTING -i eth0 -p tcp --destination-port
22 -j DNAT --to-destination 172.16.1.10:22

[root@router]# iptables -t filter -A FORWARD -i eth0 -p tcp --destination-port
22 -m state --state NEW -j ACCEPT

[root@router]# iptables -t filter -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT

[root@router]# iptables -t filter -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT

[root@router]# iptables -t filter -A OUTPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT

[root@router]# iptables -t filter -A INPUT -m state --state NEW -i lo -j
ACCEPT
```

Bước 18. [Trên máy ảo ***Private Server***] Cấu hình Default Gateway trỏ đến *eth1* của ***Router*** và kiểm tra kết nối đến máy thật Windows ***Client***

```
[root@priv-server]# route add default gw 172.16.1.1
[root@priv-server]# ping 192.168.1.100
64 bytes from 192.168.1.100: icmp_seq=1 ttl=128 time=1.251 ms
```

Kiểm tra hoạt động và lưu lại cấu hình của iptables

Bước 19. Liệt kê các rule của ***iptables*** và lưu lại cấu hình này

```
[root@router]# iptables -L -t nat
[root@router]# iptables -L -t filter
[root@router]# iptables -L -t mangle
[root@router]# iptables-save > /etc/sysconfig/fwrules.saved
```

Bước 20. Khởi động lại dịch vụ ***iptables*** và nạp lại các rule

```
[root@router]# service iptables restart
[root@router]# iptables-restore < /etc/sysconfig/fwrules.saved
```

Bước 21. Kiểm tra các kết nối theo bảng cấu hình firewall bên dưới để đảm bảo cấu hình đã chính xác.

Kết nối đến / Kết nối từ	Private Server	Router	Windows Client
Private Server	n/a	DNS, SSH, PING	ALL
Router	SSH	n/a	DNS, SSH, PING
Windows Client	SSH, HTTP	SSH	n/a