

# **HỌC VIỆN KỸ THUẬT MẬT MÃ**

**KHOA AN TOÀN THÔNG TIN**



**BÀI THỰC HÀNH SỐ 01**

## **THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES**

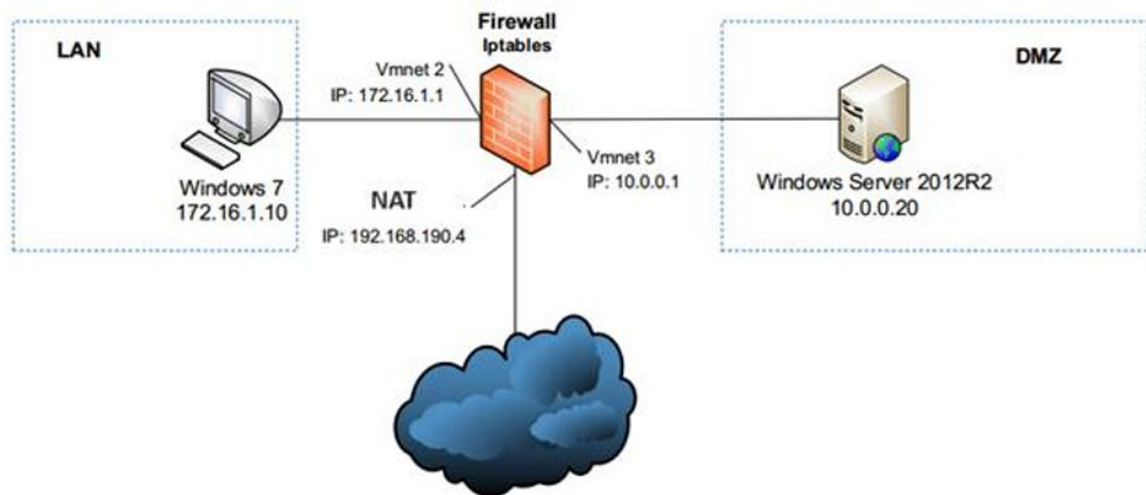
**Sinh viên thực hiện: Nguyễn Hữu Văn – AT190157**

**Hà Nội, 2025**

# Mục Lục

I. Mô hình cài đặt: .....	3
II. Các kịch bản thực hiện .....	9
Kịch bản 1: Cho phép máy tính trong LAN ping ra ngoài mạng Internet.....	9
Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet.....	10
Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet.....	11
Kịch bản 4. Cho phép cập tới máy chủ web trong phân vùng mạng DMZ ....	12
Trường hợp 1: Cho phép máy tính trong mạng LAN truy cập tới website trong mạng DMZ.....	13
Trường hợp 2: Cho phép kết nối từ Internet vào máy chủ web (từ máy vật lý vào DMZ).....	15
Kịch bản 5. Cho phép người dùng gửi và nhận thư điện tử.....	18
III. Kết luận: .....	21

## I. Mô hình cài đặt:



### Các card mạng:

Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.101.0
VMnet2	Host-only	-	Connected	-	172.16.1.0
VMnet3	Host-only	-	Connected	-	10.0.0.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.162.0

Buttons: Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
Bridged to:  Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

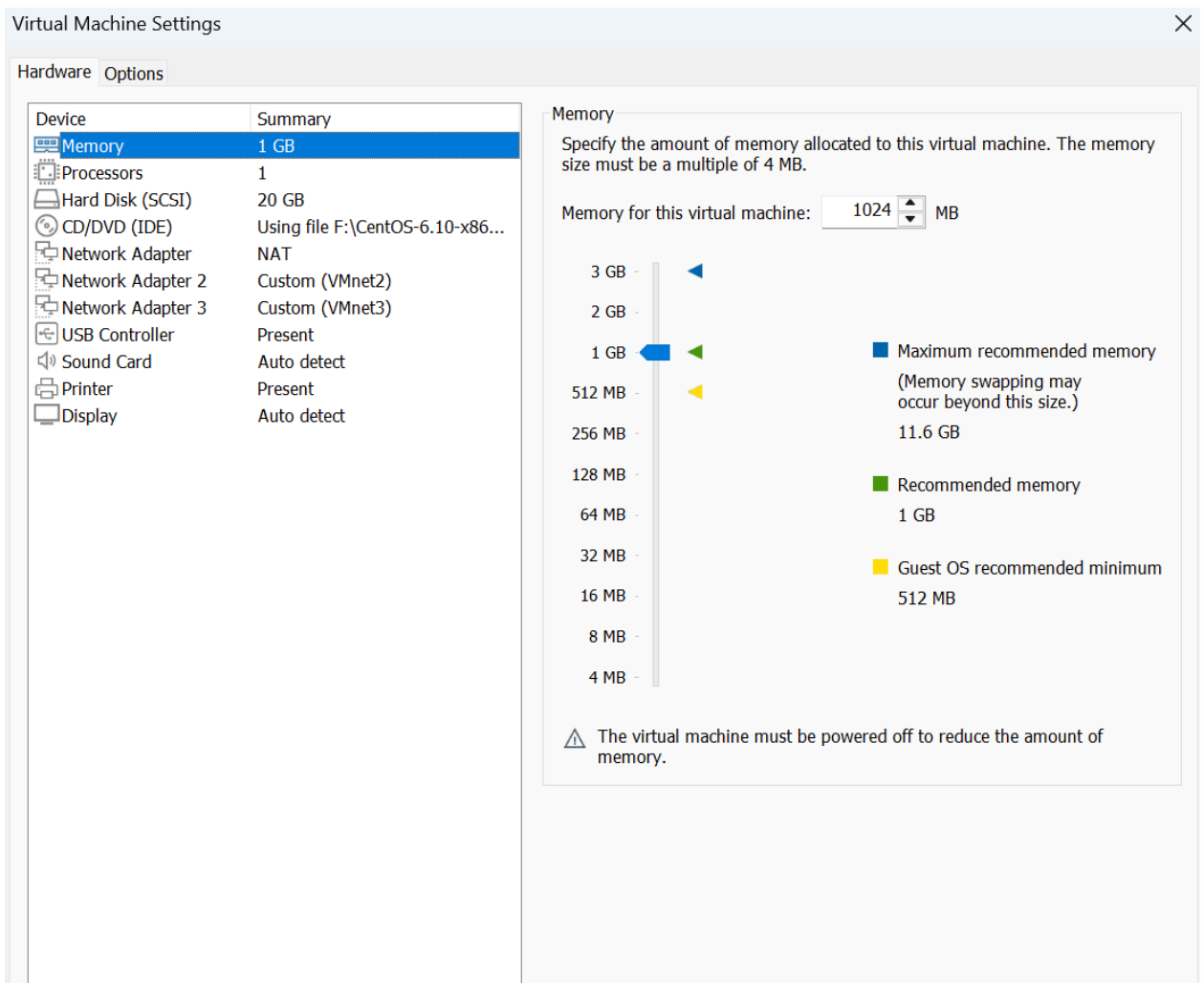
☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network  
Host virtual adapter name: VMware Network Adapter VMnet1

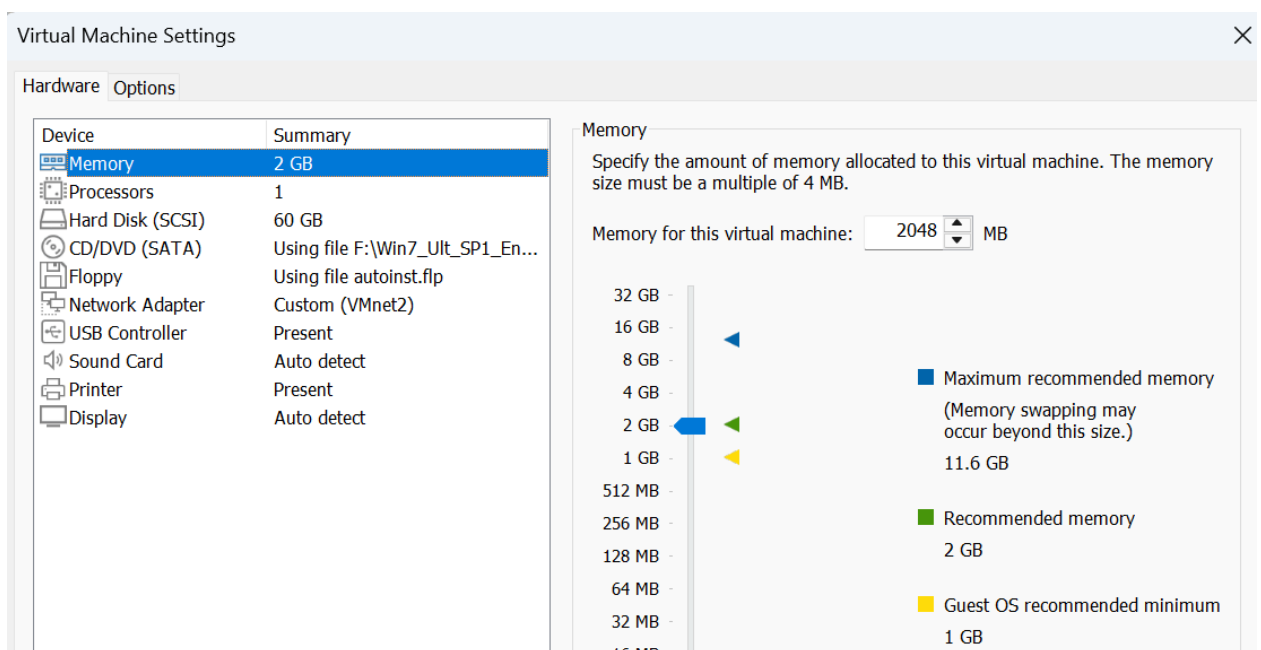
☒ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP:  Subnet mask:

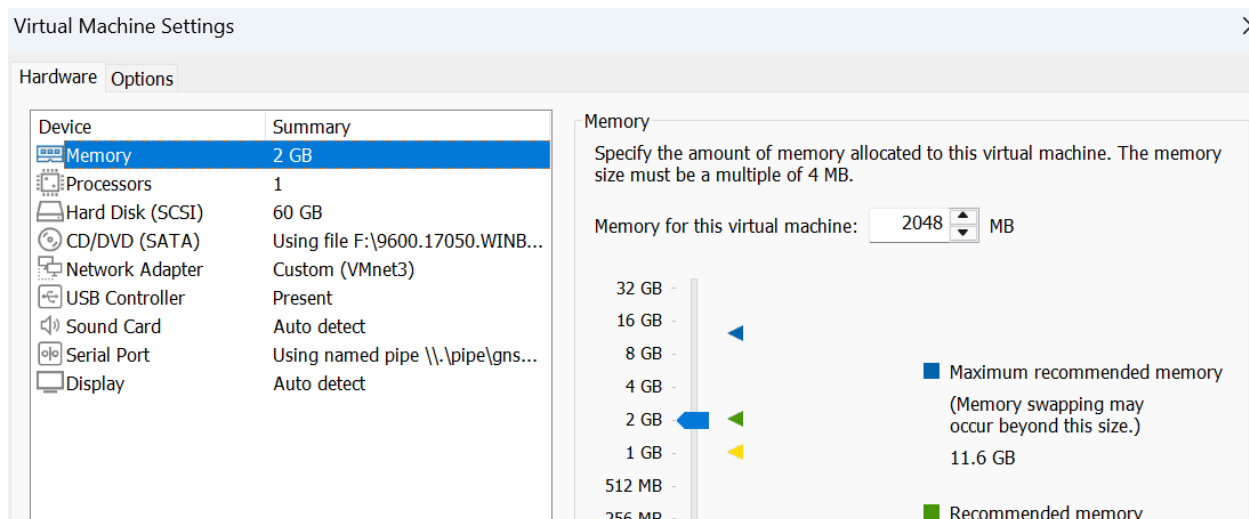
### Cấu hình máy ảo Centos:



## Cấu hình máy ảo Windows 7:



## Cấu hình máy ảo Windows server 2012:



Cấu hình IP trên Centos (eth0 là mạng NAT, eth1 là mạng VMnet2, eth2 là mạng VMnet3)

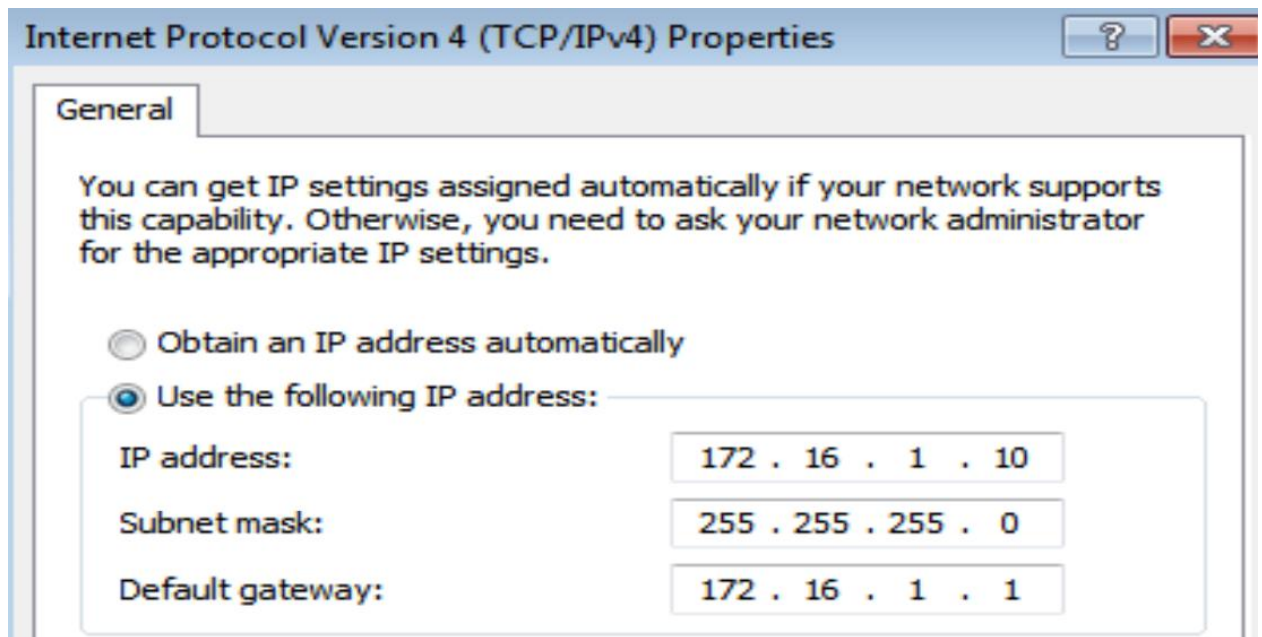
```
[root@localhost Desktop]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:A9:E5:34
          inet addr:192.168.162.165  Bcast:192.168.162.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea9:e534/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7532 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1185 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2456740 (2.3 MiB)  TX bytes:130556 (127.4 KiB)

eth1      Link encap:Ethernet  HWaddr 00:0C:29:A9:E5:3E
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea9:e53e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1684 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2069 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:180716 (176.4 KiB)  TX bytes:2123592 (2.0 MiB)

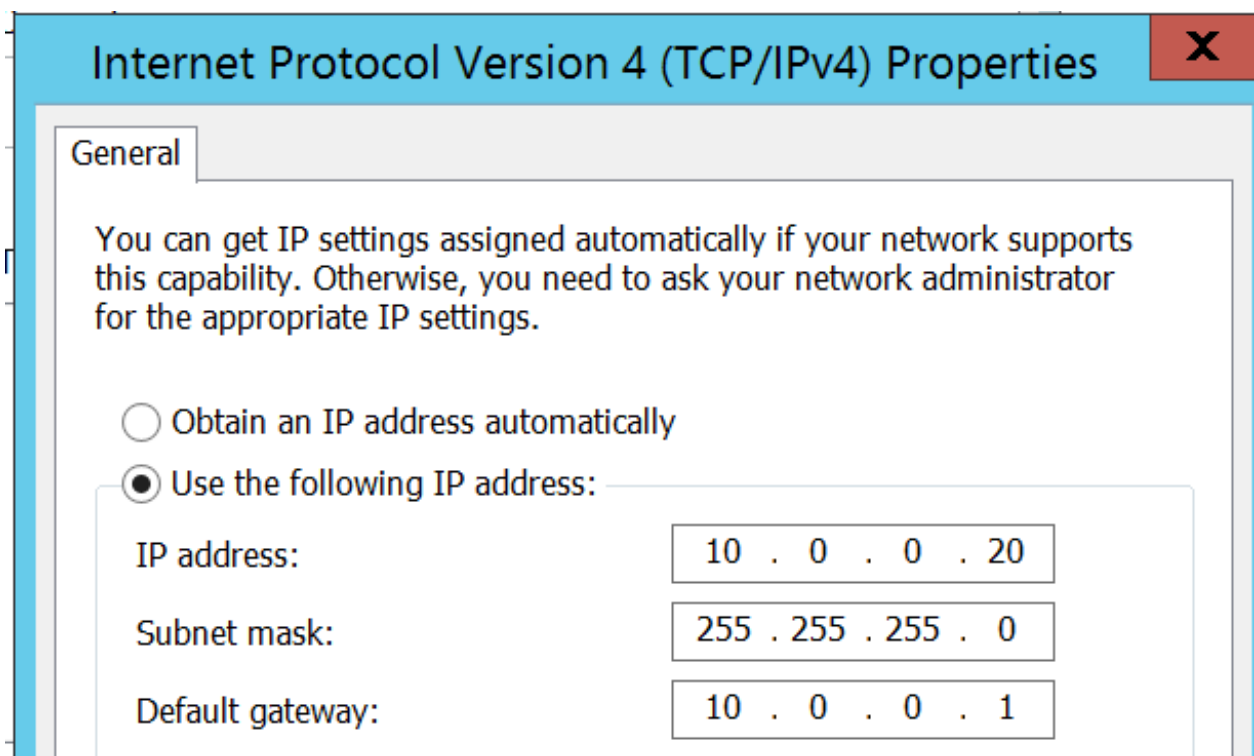
eth2      Link encap:Ethernet  HWaddr 00:0C:29:A9:E5:48
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea9:e548/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:12089 (11.8 KiB)  TX bytes:878 (878.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
```

Cấu hình IP trên Win 7:



Cấu hình IP trên Win server 2012:



Kiểm tra từ Centos ping tới các máy:

```
[root@localhost Desktop]# ping 8.8.8.8
connect: Network is unreachable
[root@localhost Desktop]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=27.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=27.4 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1438ms

[root@localhost Desktop]# ping 172.16.1.10 -c 3
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.478 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.445 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.443 ms

--- 172.16.1.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms

[root@localhost Desktop]# ping 10.0.0.20 -c 2
PING 10.0.0.20 (10.0.0.20) 56(84) bytes of data.
64 bytes from 10.0.0.20: icmp_seq=1 ttl=128 time=0.652 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=128 time=0.400 ms

--- 10.0.0.20 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
```

Xem trạng thái iptables:

```
[root@localhost Desktop]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination          state RELATED,
ESTABLISHED
1  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0
2  ACCEPT        icmp --  0.0.0.0/0              0.0.0.0/0
3  ACCEPT        all  --  0.0.0.0/0              0.0.0.0/0
4  ACCEPT        tcp  --  0.0.0.0/0              0.0.0.0/0            state NEW tcp
dpt:22
5  REJECT        all  --  0.0.0.0/0              0.0.0.0/0            reject-with ic
mp-host-prohibited

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination          reject-with ic
mp-host-prohibited
1  REJECT        all  --  0.0.0.0/0              0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
```

Xóa các rules trong table filter và table nat của iptables:



```
[root@localhost Desktop]# iptables -t filter -F
[root@localhost Desktop]# iptables -t nat -F
```

Kiểm tra lại:

```
[root@localhost Desktop]# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination

Table: filter
Chain INPUT (policy ACCEPT)
num target      prot opt source                destination

Chain FORWARD (policy ACCEPT)
num target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination
```

Chuyển iptables sang trạng thái chặn tất cả:

```
[root@localhost Desktop]# iptables -P INPUT DROP
[root@localhost Desktop]# iptables -P FORWARD DROP
[root@localhost Desktop]# iptables -P OUTPUT DROP
[root@localhost Desktop]# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination

Table: filter
Chain INPUT (policy DROP)
num target      prot opt source                destination

Chain FORWARD (policy DROP)
num target      prot opt source                destination

Chain OUTPUT (policy DROP)
num target      prot opt source                destination
```



## II. Các kịch bản thực hiện

### Kịch bản 1: Cho phép máy tính trong LAN ping ra ngoài mạng Internet

Bước 1: Kiểm tra kết nối trên máy Win7 khi ping đến 1 địa chỉ bất kỳ không ping được ra ngoài Internet

```
C:\Users\at190157>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
    Control-C
^C
```

Kết quả: không ping được ra ngoài Internet

Bước 2. Thiết lập luật trên tường lửa Iptables để cho phép máy trạm Ping ra bên ngoài.

```
[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth0 -s 172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth0 -o eth1 -d 172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
```

```
[root@localhost Desktop]# iptables -t nat -A POSTROUTING -o eth0 -s 172.16.1.0/24 -j SNAT --to-source 192.168.162.165
```

Sửa file /proc/sys/net/ipv4/ip\_forward

```
at190157@localhost:/home/at190157/Desktop
File Edit View Search Terminal Help
GNU nano 2.0.9 File: /proc/sys/net/ipv4/ip_forward
```

1

Kiểm tra lại trạng thái tường lửa

```
[root@localhost Desktop]# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num target      prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
num target      prot opt source                destination
1    SNAT          all  -- 172.16.1.0/24          0.0.0.0/0            to:192.168.162.165

Chain OUTPUT (policy ACCEPT)
num target      prot opt source                destination

Table: filter
Chain INPUT (policy DROP)
num target      prot opt source                destination

Chain FORWARD (policy DROP)
num target      prot opt source                destination
1    ACCEPT         icmp -- 172.16.1.0/24          0.0.0.0/0            icmp type 255
2    ACCEPT         icmp -- 0.0.0.0/0              172.16.1.0/24        icmp type 255

Chain OUTPUT (policy DROP)
num target      prot opt source                destination
```

Trên máy Win 7 thực hiện ping ra ngoài mạng

```
C:\Users\at190157>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=23ms TTL=127
Reply from 8.8.8.8: bytes=32 time=23ms TTL=127
Reply from 8.8.8.8: bytes=32 time=24ms TTL=127
Reply from 8.8.8.8: bytes=32 time=23ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 24ms, Average = 23ms
```

Thành công

## Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet

Bước 1. Kiểm tra truy vấn: Trước khi thiết lập luật cho tường lửa, tại máy trạm Windows 7 không truy vấn được DNS. Sử dụng lệnh nslookup để truy vấn.

```
C:\Users\at190157>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server: UnKnown
Address: 8.8.8.8
```

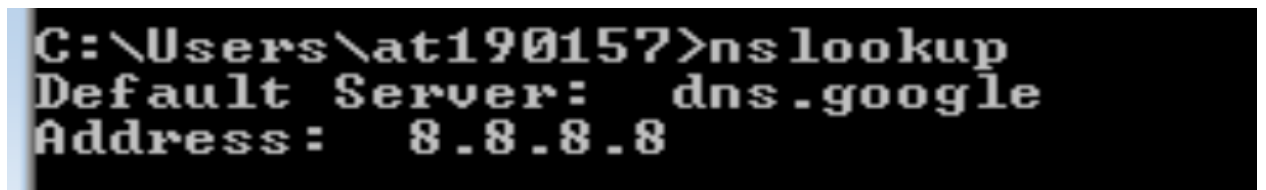
Bước 2. Cấu hình luật để cho phép truy vấn DNS tại tường lửa.

```
[root@localhost Desktop]# #iptables -A FORWARD -i eth1 -o eth0 -s 172.16.1.0/24 -p udp --dport 53 -j ACCEPT
[root@localhost Desktop]# #iptables -A FORWARD -i eth0 -o eth1 -d 172.16.1.0/24 -p udp --dport 53 -j ACCEPT
```

## Kiểm tra lại tường lửa

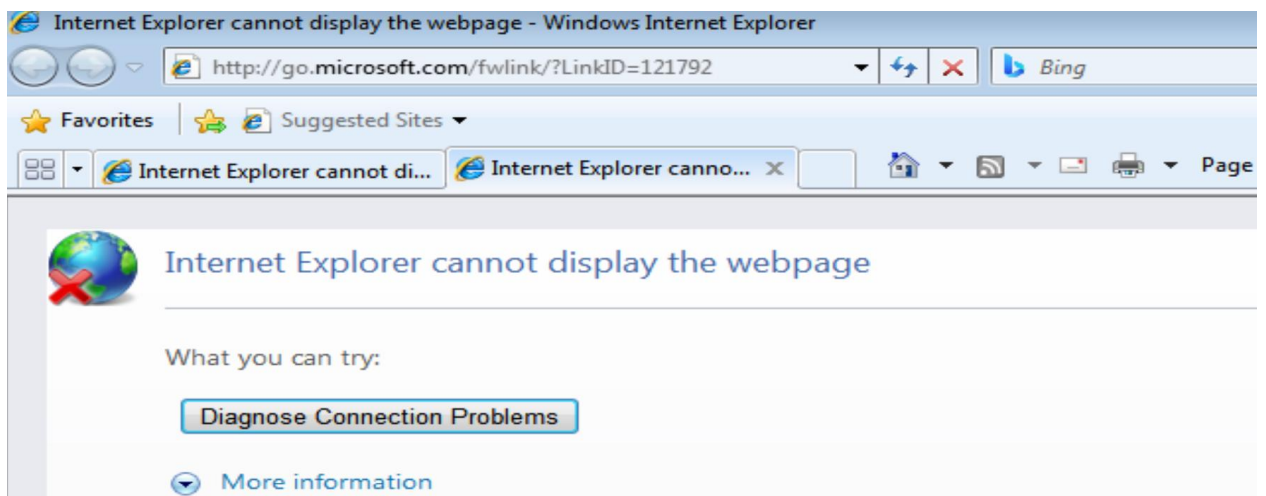
```
Chain FORWARD (policy DROP)
num target      prot opt source                destination            icmp type 255
1  ACCEPT        icmp -- 172.16.1.0/24          0.0.0.0/0              icmp type 255
2  ACCEPT        icmp -- 0.0.0.0/0              172.16.1.0/24          icmp type 255
3  ACCEPT        udp  -- 172.16.1.0/24          0.0.0.0/0              udp dpt:53
4  ACCEPT        udp  -- 0.0.0.0/0              172.16.1.0/24          udp dpt:53
```

## Bước 3. Kiểm tra kết quả



## Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet

Bước 1: Kiểm tra truy cập Tại máy Windows 7 sử dụng trình duyệt web truy cập vào website bất kỳ, kết quả không truy cập được



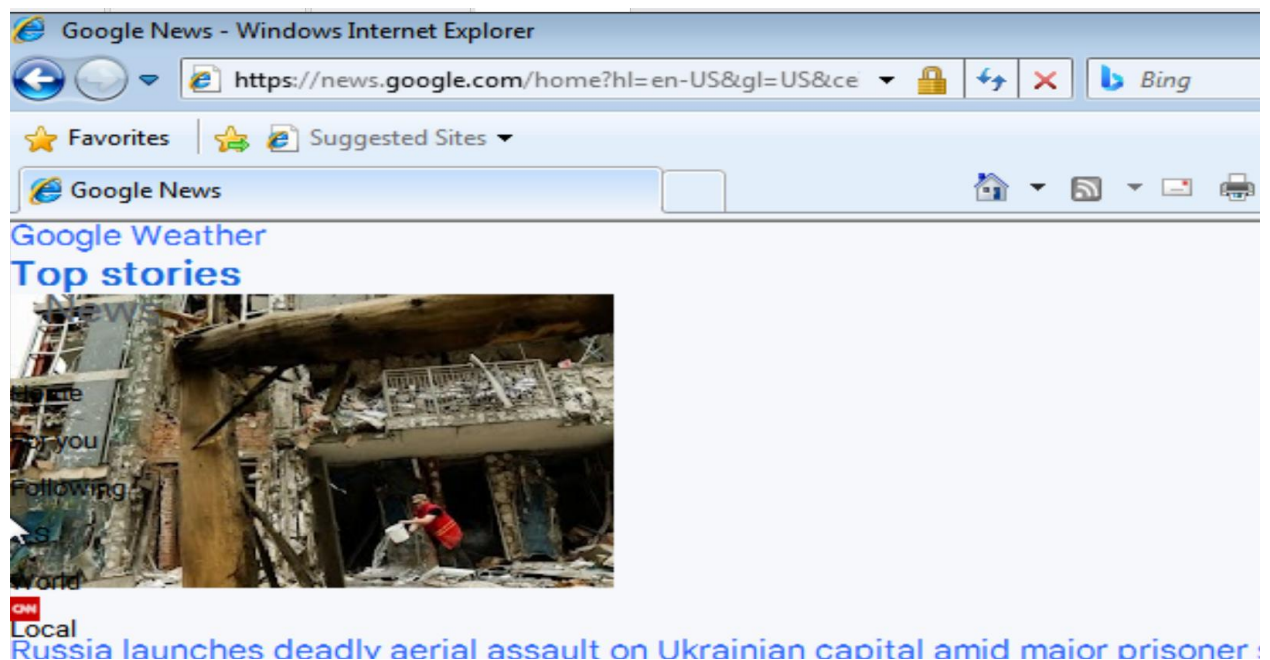
Bước 2. Cấu hình trên tường lửa Iptables để cho phép máy trạm truy cập website qua hai giao thức HTTP và HTTPS.

```
[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth0 -s 172.16.1.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth0 -o eth1 -d 172.16.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT
```

## Kiểm tra luật

num	target	prot	opt	source	destination	
1	ACCEPT	icmp	--	172.16.1.0/24	0.0.0.0/0	icmp type 255
2	ACCEPT	icmp	--	0.0.0.0/0	172.16.1.0/24	icmp type 255
3	ACCEPT	udp	--	172.16.1.0/24	0.0.0.0/0	udp dpt:53
4	ACCEPT	udp	--	0.0.0.0/0	172.16.1.0/24	udp dpt:53
5	ACCEPT	tcp	--	172.16.1.0/24	0.0.0.0/0	multiport dports 80,443
6	ACCEPT	tcp	--	0.0.0.0/0	172.16.1.0/24	multiport sports 80,443

Bước 3. Kiểm tra kết quả Trở lại máy Windows 7 sử dụng trình duyệt truy cập website, kết quả thành công.

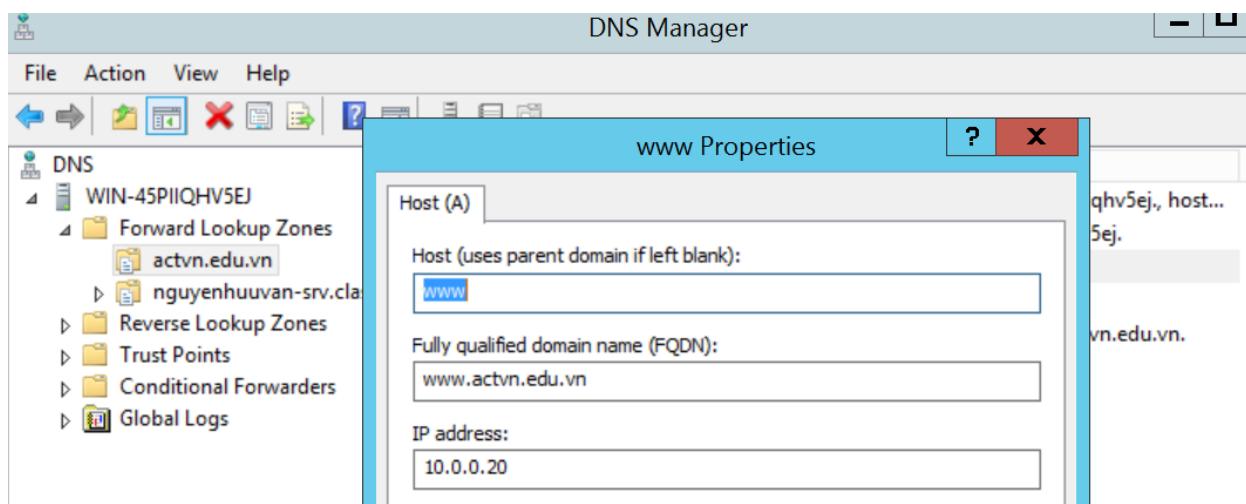


## Kịch bản 4. Cho phép cập tới máy chủ web trong phân vùng mạng DMZ

Bước 1. Chuẩn bị

- Trên máy chủ Windows Server 2012 đã cài đặt sẵn máy chủ web IIS với trang web mặc định của Windows.

- Cài đặt sẵn dịch vụ phân giải tên miền DNS với tên: [www.actvn.edu.vn](http://www.actvn.edu.vn)



## Bước 2. Cấu hình luật

### Trường hợp 1: Cho phép máy tính trong mạng LAN truy cập tới website trong mạng DMZ

Cấu hình mạng trên Windows 7:

☒ Use the following IP address:

IP address:	172 . 16 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	172 . 16 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:	8 . 8 . 8 . 8
Alternate DNS server:	. . .

Hình trên khai báo địa chỉ IP của máy chủ phân giải tên miền Google để máy chủ có thể truy cập ra Internet. Để Windows 7 có thể truy cập tới website trong DMZ thì cần khai báo vào file hosts như sau (sử dụng quyền Administrator):

C:\Windows\System32\drivers\etc

```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost

10.0.0.20      www.actvn.edu.vn
```

Cấu hình luật trên tường lửa Iptables kiểm tra truy vấn tên miền website tới máy chủ DNS trong vùng mạng DMZ:

```
[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth2 -s 172.16.1.0/24 -p udp --dport 53 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth1 -d 172.16.1.0/24 -p udp --sport 53 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth2 -s 172.16.1.0/24 -p icmp -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth1 -d 172.16.1.0/24 -p icmp -j ACCEPT
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth1 -d 192.168.162.165 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20:80
[root@localhost Desktop]# iptables -t nat -A POSTROUTING -o eth2 -s 172.16.1.0/24 -j SNAT --to-source 10.0.0.1
```

Tại máy Windows 7 kiểm tra kết quả:

```
C:\Users\at190157>ping www.actvn.edu.vn

Pinging www.actvn.edu.vn [10.0.0.20] with 32 bytes of data:
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127

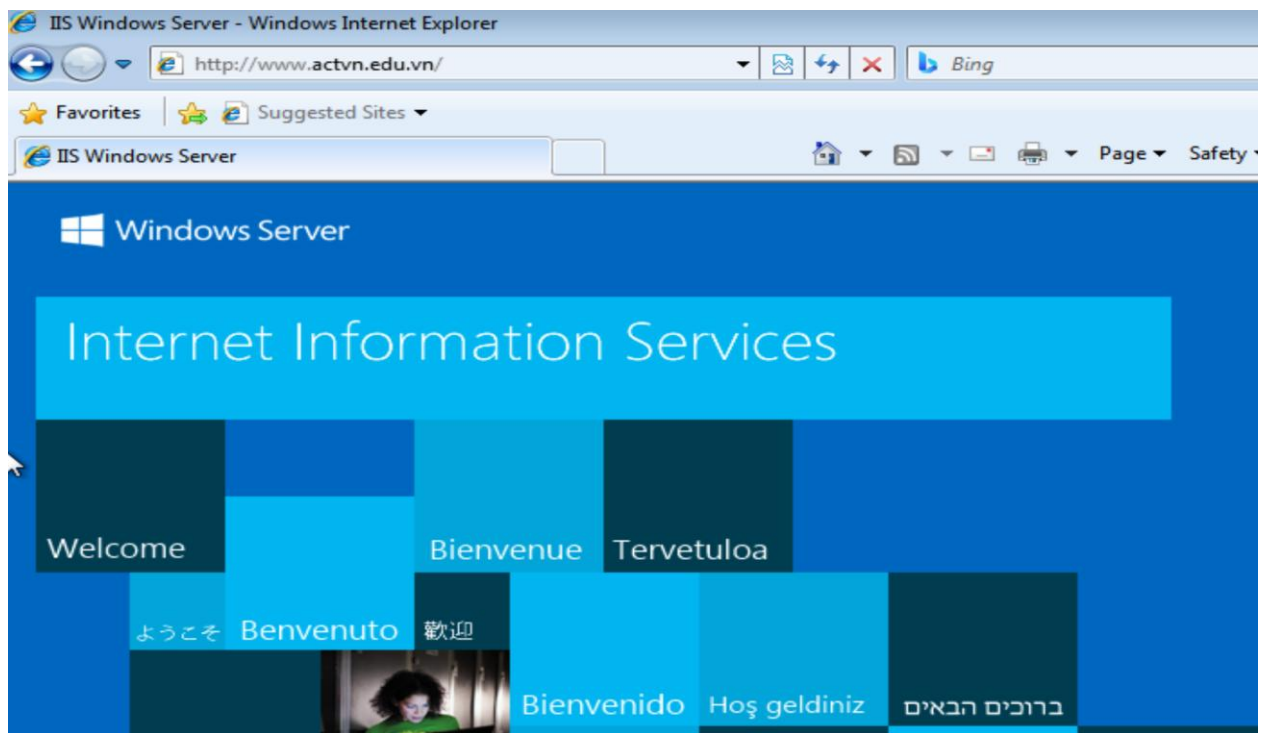
Ping statistics for 10.0.0.20:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Máy Windows 7 truy vấn tên miền tới máy chủ DNS trong DMZ thành công.  
Tạo luật Iptables cho phép truy cập website thông qua cổng 80 của trình duyệt web:

```
[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth2 -s 172.16.1.0/24 -p tcp --dport 80 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth1 -d 172.16.1.0/24 -p tcp --sport 80 -j ACCEPT
```

Tại máy Windows 7 sử dụng trình duyệt web truy cập website trong DMZ bằng tên miền:





Kết quả thành công.

Kiểm tra luật:

7	ACCEPT	udp	--	172.16.1.0/24	0.0.0.0/0	udp dpt:53
8	ACCEPT	udp	--	0.0.0.0/0	172.16.1.0/24	udp spt:53
9	ACCEPT	icmp	--	172.16.1.0/24	0.0.0.0/0	
10	ACCEPT	icmp	--	0.0.0.0/0	172.16.1.0/24	
11	ACCEPT	tcp	--	172.16.1.0/24	0.0.0.0/0	tcp dpt:80
12	ACCEPT	tcp	--	0.0.0.0/0	172.16.1.0/24	tcp spt:80

Chain POSTROUTING (policy ACCEPT)						
num	target	prot	opt	source	destination	
1	SNAT	all	--	172.16.1.0/24	0.0.0.0/0	to:192.168.162.165
2	SNAT	all	--	172.16.1.0/24	0.0.0.0/0	to:10.0.0.1

## Trường hợp 2: Cho phép kết nối từ Internet vào máy chủ web (từ máy vật lý vào DMZ)

Từ máy vật lý, sử dụng trình duyệt web truy cập vào địa chỉ IP của giao diện mạng eth0 (kết nối Internet) trên Iptables. Kết quả không truy cập được.





## Không thể truy cập trang web này

192.168.162.165 đã từ chối kết nối.

Hãy thử:

- Kiểm tra kết nối
- [Kiểm tra proxy và tường lửa](#)

ERR\_CONNECTION\_REFUSED

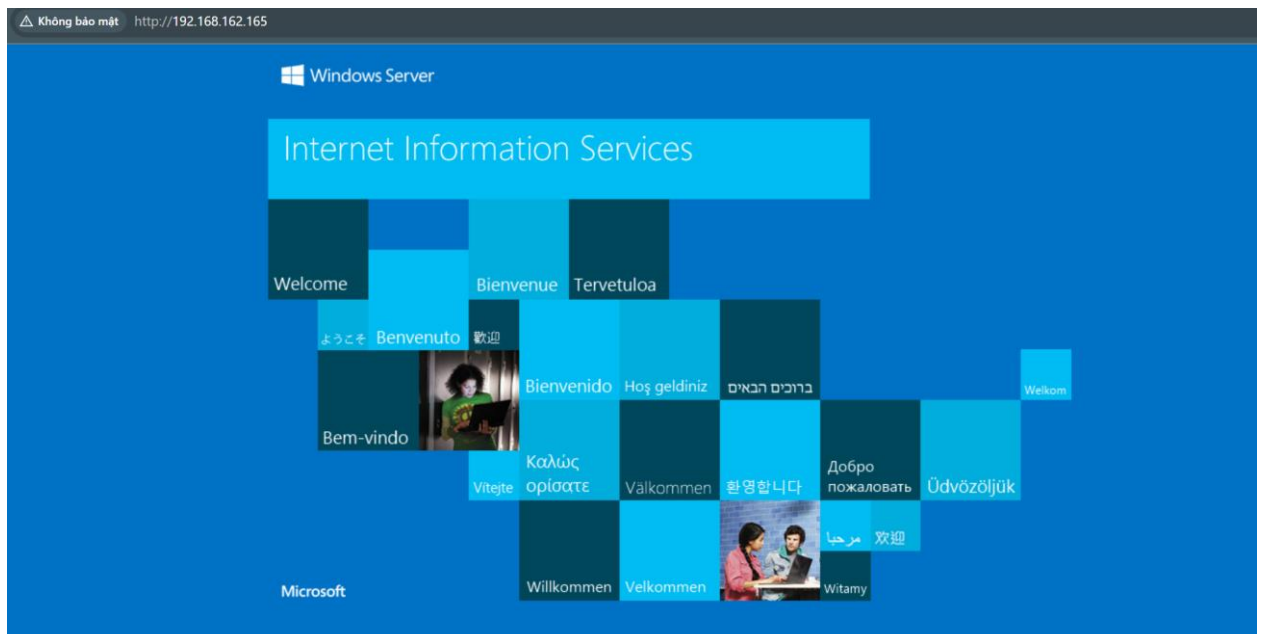
Tải lại

Chi tiết

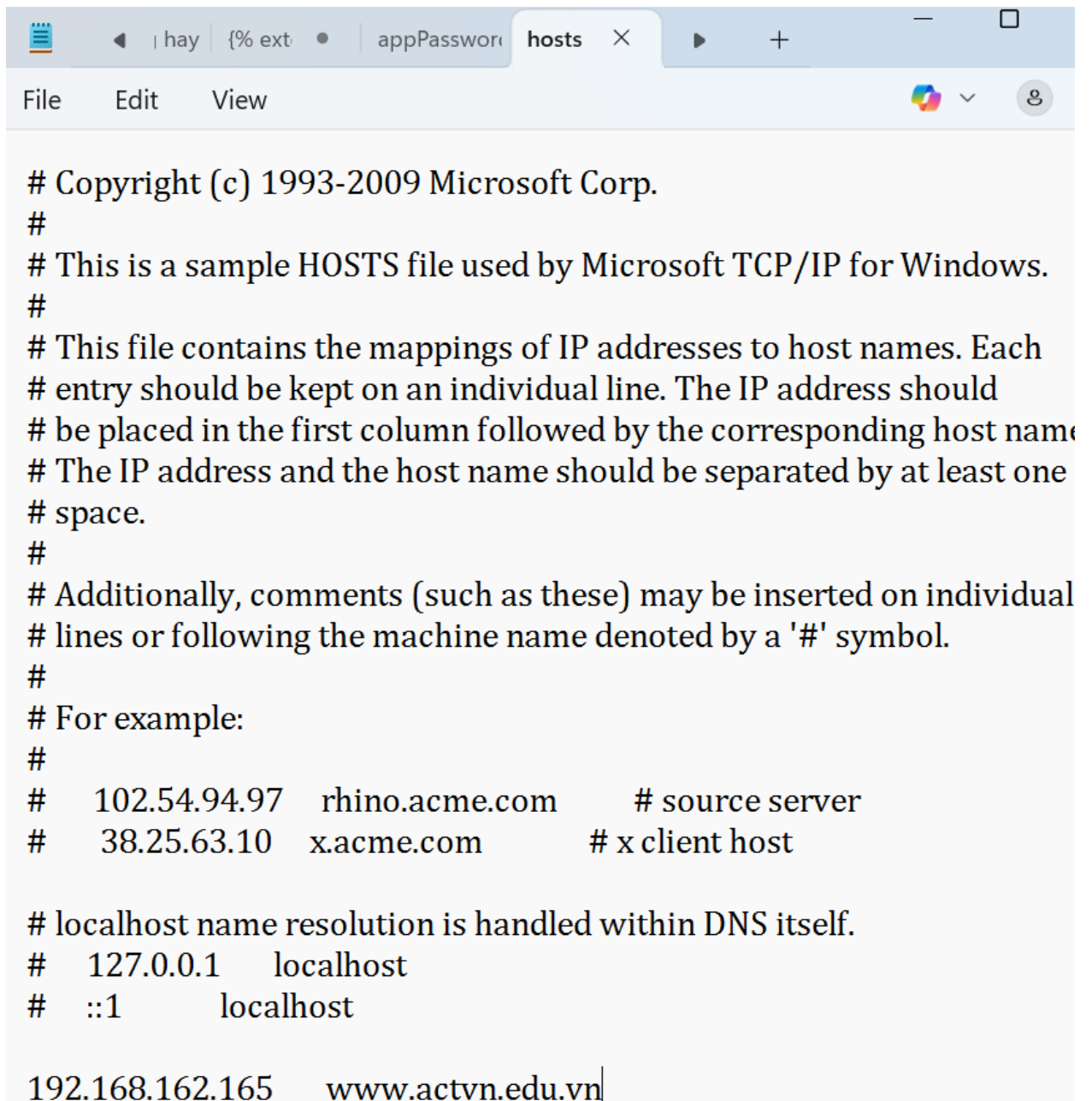
### Bước 3. Thiết lập luật trên Iptables để cho phép kết nối.

```
[root@localhost Desktop]# iptables -A FORWARD -i eth0 -o eth2 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth0 -s 10.0.0.20 -p tcp --sport 80 -j ACCEPT
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20:80
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to-destination 10.0.0.20:53
```

### Bước 4. Kết quả Từ máy vật lý, sử dụng trình duyệt web truy cập vào địa chỉ IP của giao diện mạng eth0 (kết nối Internet) trên Iptables. Kết quả thành công.

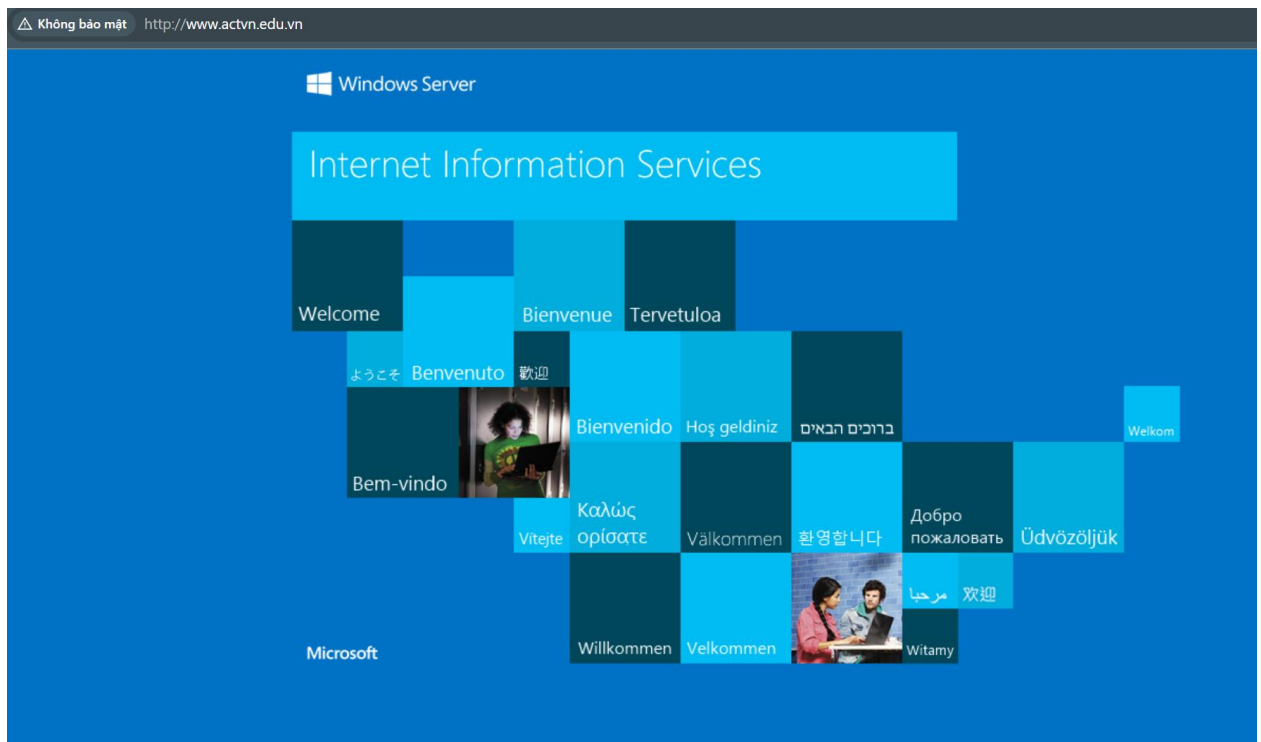


### Bước 5. Để người dùng có thể truy cập được qua tên miền. Chỉnh sửa tệp tin theo đường dẫn: C:\Windows\System32\drivers\etc\host với nội dung như sau:



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
#
192.168.162.165 www.actvn.edu.vn
```

Sử dụng trình duyệt web truy cập bằng tên miền



Kết quả máy vật lý truy cập website trong mạng DMZ thành công. Kiểm tra luật:

```

13  ACCEPT  tcp  --  0.0.0.0/0          10.0.0.20          tcp dpt:80
14  ACCEPT  tcp  --  10.0.0.20          0.0.0.0/0          tcp spt:80

```

```

Table: nat
Chain PREROUTING (policy ACCEPT)
num target prot opt source destination
1 DNAT tcp -- 0.0.0.0/0 192.168.162.165 tcp dpt:80 to:10.0.0.20:80

```

## Kịch bản 5. Cho phép người dùng gửi và nhận thư điện tử

Cấu hình trên máy Windows 7 Cấu hình phân giải tên miền trong file Hosts:

```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host nam
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
10.0.0.20                www.actvn.edu.vn
10.0.0.20                mail.actvn.edu.vn

```

### Cấu hình rule cho phép gửi nhận thư

```

[root@localhost Desktop]# iptables -A FORWARD -i eth1 -o eth2 -s 172.16.1.0/24 -p tcp -m multiport --dport 25,110 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth1 -d 172.16.1.0/24 -p tcp -m multiport --sport 25,110 -j ACCEPT

```

✓ The following settings were found by probing the given server:

**Server settings**  
**INCOMING SERVER**  
Protocol: POP3  
Hostname: mail.actvn.edu.vn  
Port: 110  
Connection security: None  
Authentication method: Normal password  
Username: user1

**OUTGOING SERVER**  
Hostname: mail.actvn.edu.vn  
Port: 25  
Connection security: None  
Authentication method: Encrypted password  
Username: user1

[Advanced config](#)

### Bước 3. Cấu hình trên máy Vật lý

```

# localhost name resolution is handled within DNS itself.
# 127.0.0.1    localhost
# ::1         localhost

192.168.162.165    www.actvn.edu.vn
192.168.162.165    mail.actvn.edu.vn

```

Cấu hình luật tường lửa Iptables để cho phép ứng dụng mail tại máy vật lý truy cập tới máy chủ thư:

```
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -d 192.168.162.165 -p tcp --dport 110 -j DNAT --to-destination 10.0.0.20:110
[root@localhost Desktop]# iptables -t nat -A PREROUTING -i eth0 -d 192.168.162.165 -p tcp --dport 25 -j DNAT --to-destination 10.0.0.20:25

[root@localhost Desktop]# iptables -A FORWARD -i eth0 -o eth2 -d 10.0.0.20 -p tcp -m multiport --dport 25,110 -j ACCEPT
[root@localhost Desktop]# iptables -A FORWARD -i eth2 -o eth0 -s 10.0.0.20 -p tcp -m multiport --sport 25,110 -j ACCEPT
```

Bật ứng dụng thư Thunderbird, cấu hình và ấn re-test. Kết quả thành công.

✓ The following settings were found by probing the given server:

**Manual configuration**

**INCOMING SERVER**

Protocol: POP3

Hostname: mail.actvn.edu.vn

Port: 110

Connection security: None

Authentication method: Normal password

Username: user2

**OUTGOING SERVER**

Hostname: mail.actvn.edu.vn

Port: 25

Connection security: None

Authentication method: Encrypted password

Username: user2

Advanced config

Kiểm tra luật:

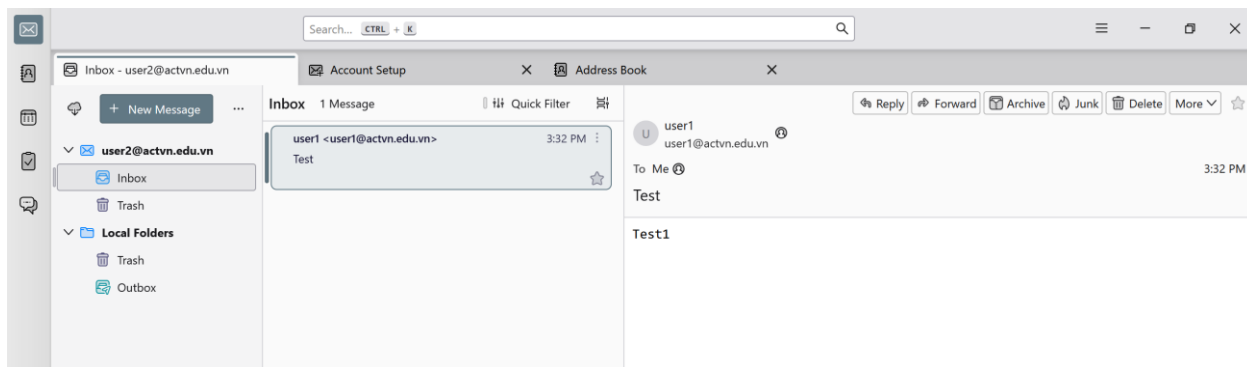
15	ACCEPT	tcp	--	172.168.1.0/24	0.0.0.0/0	multiport dports 25,110
16	ACCEPT	tcp	--	0.0.0.0/0	172.168.1.0/24	multiport sports 25,110
17	ACCEPT	tcp	--	0.0.0.0/0	10.0.0.20	multiport dports 25,110
18	ACCEPT	tcp	--	10.0.0.20	0.0.0.0/0	multiport sports 25,110

Bước 4. Kiểm tra gửi và nhận mail

Tại máy trạm Windows 7 với tài khoản user1@actvn.edu.vn gửi thư cho user2@actvn.edu.vn tại máy vật lý:

The screenshot shows the Thunderbird 'Write: Test' window. The 'From' field is 'user1 <user1@actvn.edu.vn>'. The 'To' field is 'user2@actvn.edu.vn'. The 'Subject' field is 'Test'. The body of the email starts with 'Test1'. The window includes a menu bar (File, Edit, View, Insert, Format, Options, Tools, Help) and a toolbar with icons for Send, Encrypt, Spelling, Save, and Attach.

Tại ứng dụng mail trên máy vật lý với tài khoản User2 kiểm tra mail:



Kết quả User2 đã nhận thành công thư của User1.

### III. Kết luận:

Bài thực hành đã hướng dẫn cấu hình luật cho tường lửa Iptables để kiểm soát các dịch vụ vào ra từ mạng nội bộ tới mạng máy chủ cũng như mạng Internet. Đây là loại tường lửa miễn phí và được tích hợp sẵn trong các hệ điều hành Linux.