

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 01
**THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA
IPTABLES**

Người xây dựng bài thực hành:

ThS. Cao Minh Tuấn

HÀ NỘI, 2018

MỤC LỤC

Mục lục	2
Thông tin chung về bài thực hành.....	3
Chuẩn bị bài thực hành	4
Đối với giảng viên.....	4
Đối với sinh viên	4
THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES	5
1.1. Mô tả.....	5
1.2. Chuẩn bị.....	5
1.3. Mô hình cài đặt.....	5
1.4. Các kịch bản thực hiện	6
<i>1.4.1. Kịch bản 1. Cho phép máy tính trong LAN Ping ra ngoài mạng Internet</i>	<i>9</i>
<i>1.4.2. Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet..</i>	<i>10</i>
<i>1.4.3. Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet</i>	<i>11</i>
<i>1.4.4. Kịch bản 4. Cho phép cập tới máy chủ web trong phân vùng mạng DMZ</i>	<i>13</i>
<i>1.4.5. Kịch bản 5. Cho phép người dùng gửi và nhận thư điện tử.....</i>	<i>18</i>

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Thiết lập và cấu hình tường lửa Iptables.

Học phần: An toàn mạng máy tính

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

Máy tính vật lý có cấu hình tối thiểu: RAM 4GB, 50 HDD

- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có
- Yêu cầu khác: máy chiếu, bảng viết, bút/phấn viết bảng

Công cụ được cung cấp cùng tài liệu này:

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

THIẾT LẬP VÀ CẤU HÌNH TƯỜNG LỬA IPTABLES

1.1. Mô tả

Tường lửa Iptables là loại tường lửa miễn phí được tích hợp sẵn trong các hệ điều hành Linux. Có thể ứng dụng để kiểm soát truy cập cho mạng máy tính nội bộ và phân vùng mạng máy chủ.

Trong bài thực hành này hướng dẫn thiết lập tập luật cho tường lửa Iptables để kiểm soát các dịch vụ cho mạng nội bộ, mạng DMZ, mạng Internet. Cụ thể là cho phép người dùng trong mạng nội bộ LAN có thể truy cập được ra ngoài Internet với các giao thức HTTP, HTTPS, ICMP, DNS.

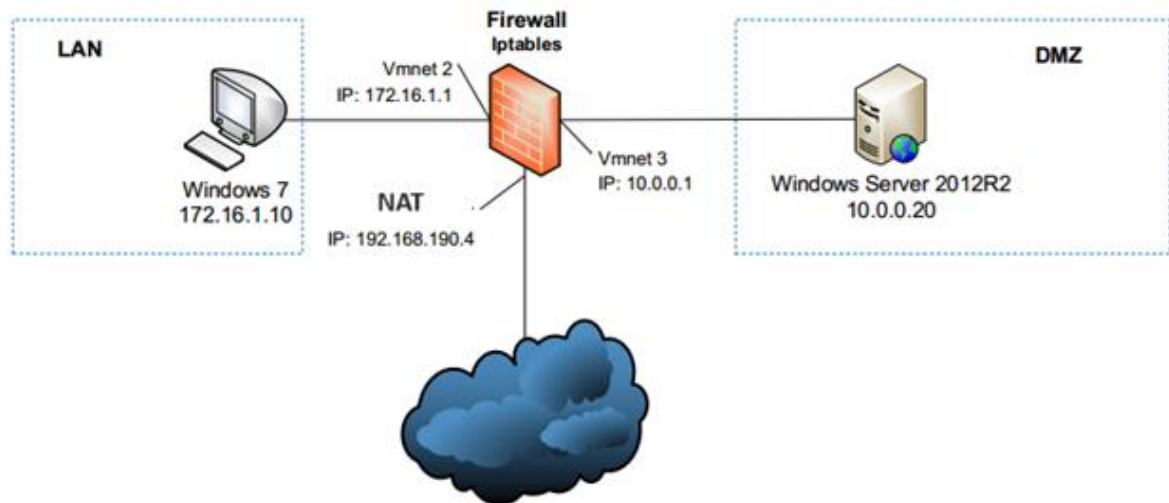
Cho phép người dùng từ mạng Internet và mạng nội bộ truy cập được trang web từ máy chủ web trong phần vùng DMZ.

Cho phép người dùng sử dụng ứng dụng thư điện tử để gửi và nhận thư với nhau.

1.2. Chuẩn bị

- 01 máy ảo hệ điều hành Windows 7: Cài đặt ứng dụng thư Mozilla Thunderbird
- 01 máy ảo hệ điều hành Windows Server 2012.
 - + Đã cài dịch vụ web sử dụng máy chủ web IIS với trang web mặc định của Microsoft.
 - + Đã cài dịch vụ phân giải tên miền DNS với các bản ghi thích hợp cho web và mail.
 - + Đã cài phần mềm máy chủ thư điện tử (MDaemon V10).
- 01 máy ảo hệ điều hành CentOS 6.5 để làm tường lửa Iptables.

1.3. Mô hình cài đặt



1.4. Các bước thực hiện

1.4.1. Bước 1. Cài đặt máy ảo

- Máy ảo Linux CentOS (Iptables)

Máy ảo có 3 cổng mạng như sau:

▼ Devices	
Memory	2 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file D:\Set...
Network Adapter	NAT
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Cổng mạng thứ 1 kết nối với switch ảo NAT nhằm mục đích vừa kết nối Internet vừa kết nối với máy vật lý.

Cổng mạng thứ 2 kết nối với switch ảo Vmnet2 kết nối với LAN ảo (Windows 7).

Cổng mạng thứ 3 kết nối với switch ảo Vmnet3 kết nối với vùng mạng DMZ có các máy chủ cung cấp dịch vụ web, mail.

Bật máy Linux để cấu hình địa chỉ IP, kết quả:

```
[attt@kattt ~]$ ifconfig
eth1      Link encap:Ethernet  HWaddr 00:0C:29:CB:80:B2
          inet addr:192.168.190.4  Bcast:192.168.190.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feeb:80b2/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19 errors:0 dropped:0 overruns:0 frame:0
          TX packets:27 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2192 (2.1 KiB)  TX bytes:1849 (1.8 KiB)
          Interrupt:19 Base address:0x2000

eth2      Link encap:Ethernet  HWaddr 00:0C:29:CB:80:BC
          inet addr:172.16.1.1  Bcast:172.16.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feeb:80bc/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:4572 (4.4 KiB)
          Interrupt:18 Base address:0x2080

eth3      Link encap:Ethernet  HWaddr 00:0C:29:CB:80:C6
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feeb:80c6/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:18 errors:0 dropped:0 overruns:0 carrier:0
```

- Cấu hình địa chỉ IP trên máy ảo 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

- Cấu hình địa chỉ IP trên máy ảo Server 2012:

☒ Use the following IP address:

IP address:	10 . 0 . 0 . 20
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 0 . 0 . 1

Kiểm tra kết nối mạng:

Từ máy ảo Linux ping tới các máy khác:

```
[attt@kattt ~]$ 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=35.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=37.0 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1465ms
rtt min/avg/max/mdev = 35.513/36.293/37.073/0.780 ms
[attt@kattt ~]$ ping 172.16.1.10
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=0.923 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=1.28 ms
^C
--- 172.16.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1145ms
rtt min/avg/max/mdev = 0.923/1.101/1.280/0.181 ms
[attt@kattt ~]$ ping 10.0.0.20
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=0.791 ms
64 bytes from 10.0.0.20: icmp_seq=2 ttl=128 time=0.669 ms
```

Kết quả máy Linux đã kết nối thành công tới các máy khác với các vùng mạng tương ứng.

1.4.2. Bước 2. Thực hiện các lệnh cơ bản

Lệnh khởi động tường lửa:

```
[root@server]# service iptables start
[root@server]# service iptables stop
[root@server]# service iptables restart
```

Để khởi động Iptables mỗi khi khởi động máy:

```
[root@server]# chkconfig iptables on
```

Để xem tình trạng của Iptables:

```
[root@server]# service iptables status
```

Lưu thông tin cấu hình:

```
[root@server]# /etc/init.d/iptables save
```

Lệnh xóa toàn bộ luật có trong Iptables:

```
[root@server]# iptables -F
[root@server]# iptables -t nat -F
```

Lệnh chuyển trạng thái mặc định của tường lửa, mặc định tường lửa Iptables đang cho phép tất cả, điều này không đảm bảo an toàn mạng. Cần thực hiện chuyển về chế độ chặn tất cả.


```
[root@katitt ~]# 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
```

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

Kiểm tra kết quả:

```
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
```

1.5. Các kịch bản thực hiện

1.5.1. Kịch bản 1. Cho phép máy tính trong LAN Ping ra ngoài mạng Internet

Bước 1. Kiểm tra kết nối trước khi thiết lập luật Iptables:

Tại máy trạm Windows 7 thực Ping đến địa chỉ IP bất kỳ.

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

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

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Kết quả, không Ping được ra ngoài mạng.

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

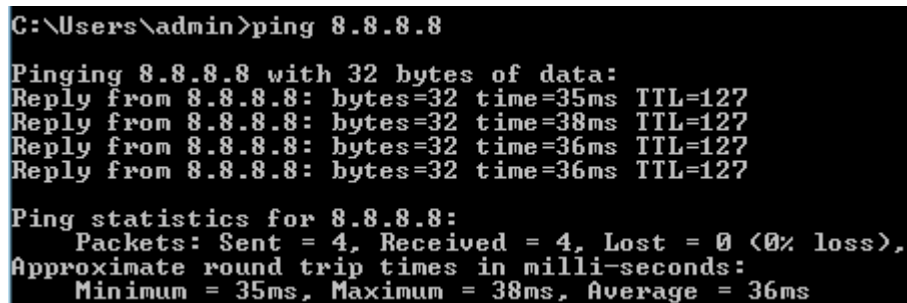
Tiếp theo đặt lệnh cho Iptables để cho phép máy trạm trong mạng nội bộ Ping ra mạng Internet.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s 172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d 172.16.1.0/24 -p icmp --icmp-type any -j ACCEPT
[root@server]#iptables -t nat -A POSTROUTING -o eth1 -s 172.16.1.0/24 -j SNAT --to-source 192.168.190.4
[root@server]#nano /proc/sys/net/ipv4/ip_forward 0 -> 1
```

Ghi chú: địa chỉ IP 192.168.190.4 là địa chỉ của giao diện mạng kết nối Internet (eth1), tùy thuộc vào trường hợp cụ thể của máy ảo mà sử dụng địa chỉ IP này.

Bước 3. Kiểm tra kết quả

Trở lại máy trạm Windows 7 kiểm tra Ping tới địa chỉ IP tại bước 1. Kết quả thành công.



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

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=35ms TTL=127
Reply from 8.8.8.8: bytes=32 time=38ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms TTL=127
Reply from 8.8.8.8: bytes=32 time=36ms 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 = 35ms, Maximum = 38ms, Average = 36ms
```

Kiểm tra luật trên tường lửa:

```
#service iptables status
```

```
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

Chain POSTROUTING (policy ACCEPT)
num target      prot opt source                destination           to:192.168.190.4
1  SNAT          all  -- 172.16.1.0/24          0.0.0.0/0
```

1.5.2. 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.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>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@server]#iptables -A FORWARD -i eth2 -o eth1 -s
172.16.1.0/24 -p udp --dport 53 -j ACCEPT

[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d
172.16.1.0/24 -p udp --sport 53 -j ACCEPT
```

Bước 3. Kiểm tra kết quả

Kết quả, lúc này tại máy Windows 7 thực hiện truy vấn thành công

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\admin>nslookup
Default Server: google-public-dns-a.google.com
Address: 8.8.8.8

> _
```

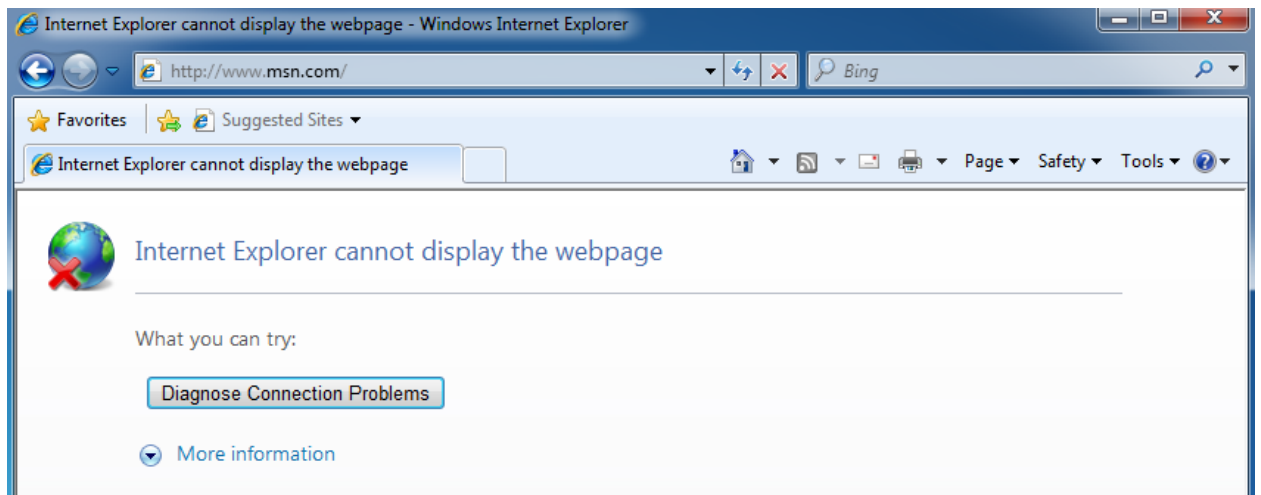
Kiểm tra luật trên tường lửa:

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 spt:53

1.5.3. 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.

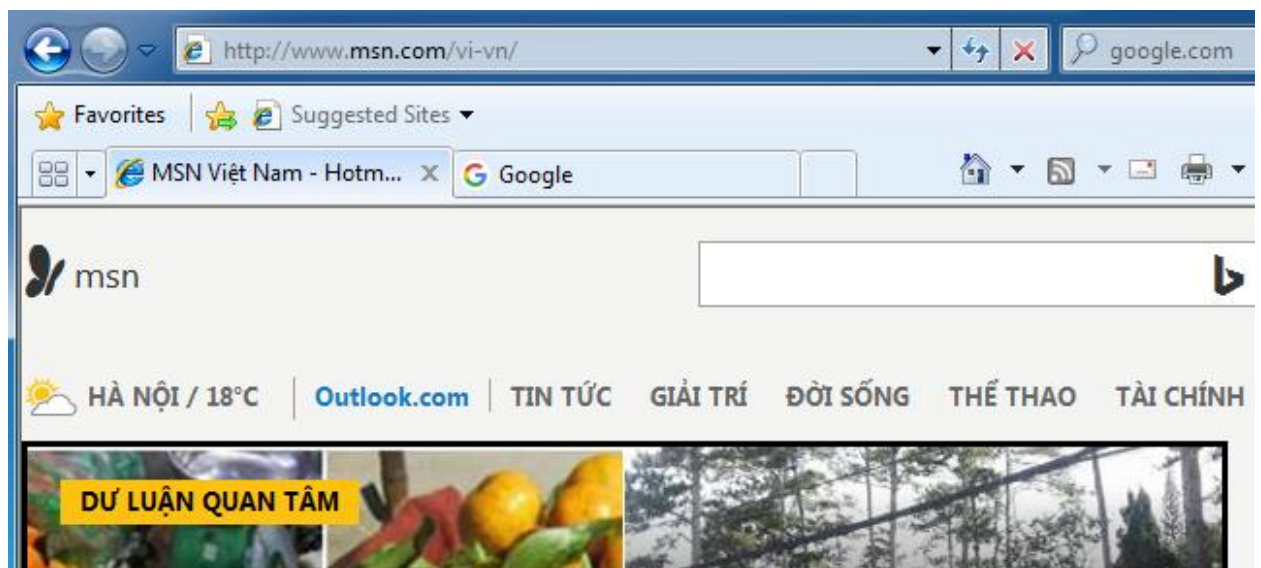


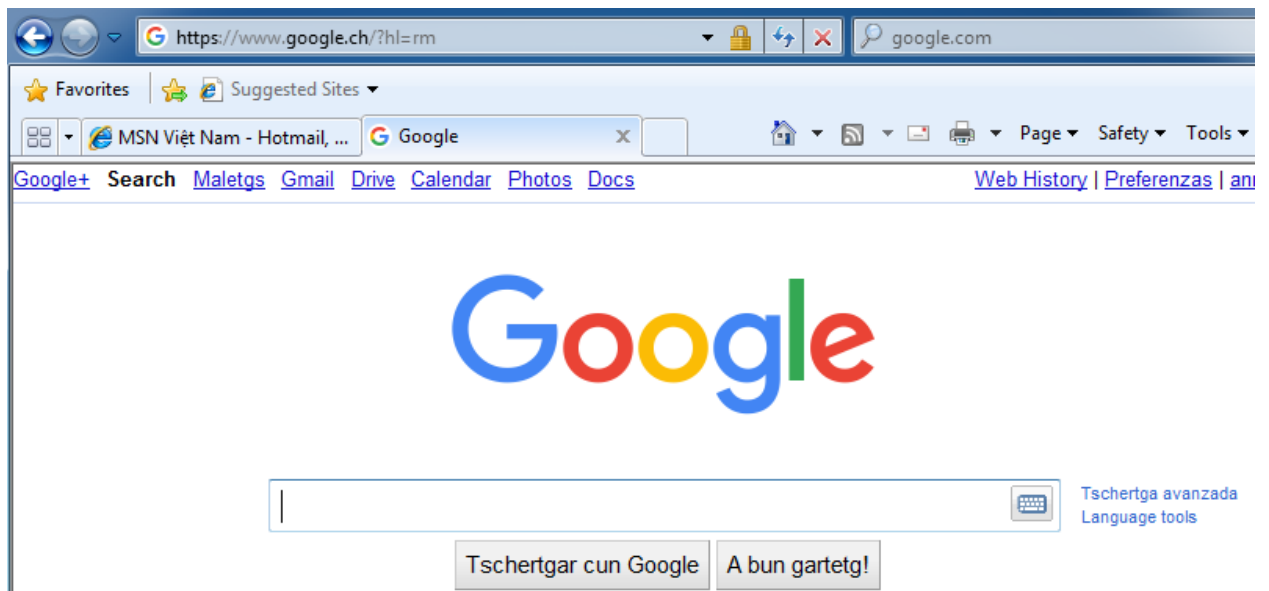
Bước 2. Cấu hình trên tường lửa Iptables để cho phép máy trạm truy cập website qua hai giao thức HTTP và HTTPS.

```
[root@server]#iptables -A FORWARD -i eth2 -o eth1 -s  
172.16.1.0/24 -p tcp -m multiport --dport 80,443 -j ACCEPT  
[root@server]#iptables -A FORWARD -i eth1 -o eth2 -d  
172.16.1.0/24 -p tcp -m multiport --sport 80,443 -j ACCEPT
```

Bước 3. Kiểm tra kết quả

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





Chú ý: Bài này phải kết hợp với kịch bản 2 để phân giải tên miền.

Kiểm tra luật:

```

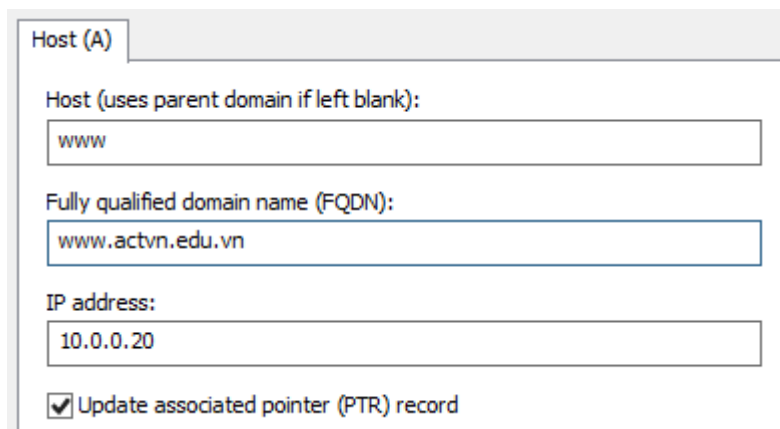
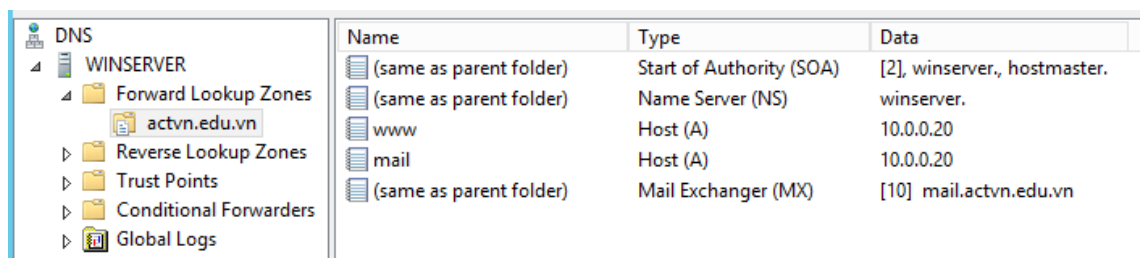
5  ACCEPT  tcp  --  172.16.1.0/24      0.0.0.0/0      multiport dports 80,443
6  ACCEPT  tcp  --  0.0.0.0/0         172.16.1.0/24  multiport sports 80,443

```

1.5.4. 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



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:

The screenshot shows the Windows 7 Network Setup Wizard. The first section is titled "Use the following IP address:" and contains three input fields: "IP address:" with the value "172 . 16 . 1 . 10", "Subnet mask:" with the value "255 . 255 . 255 . 0", and "Default gateway:" with the value "172 . 16 . 1 . 1". Below this, there are two radio buttons: "Obtain DNS server address automatically" (which is unselected) and "Use the following DNS server addresses:" (which is selected). The second section, titled "Use the following DNS server addresses:", contains two input fields: "Preferred DNS server:" with the value "8 . 8 . 8 . 8" and "Alternate DNS server:" with the value "." . . .

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

# 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:

Luật NAT:

```
[root@server]# iptables -t nat -A POSTROUTING -o eth3 -s 172.16.1.0/24 -j SNAT --to-source 10.0.0.1
```

Luật lọc Filter:

```
[root@server]# iptables -A FORWARD -i eth2 -o eth3 -s 172.16.1.0/24 -p udp --dport 53 -j ACCEPT
[root@server]# iptables -A FORWARD -i eth3 -o eth2 -d 172.16.1.0/24 -p udp --sport 53 -j ACCEPT
[root@server]# iptables -A FORWARD -i eth2 -o eth3 -s 172.16.1.0/24 -p ICMP -j ACCEPT
```

```
[root@server]# iptables -A FORWARD -i eth3 -o eth2 -d 172.16.1.0/24 -p ICMP -j ACCEPT
```

Tại máy Windows 7 kiểm tra kết quả:

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

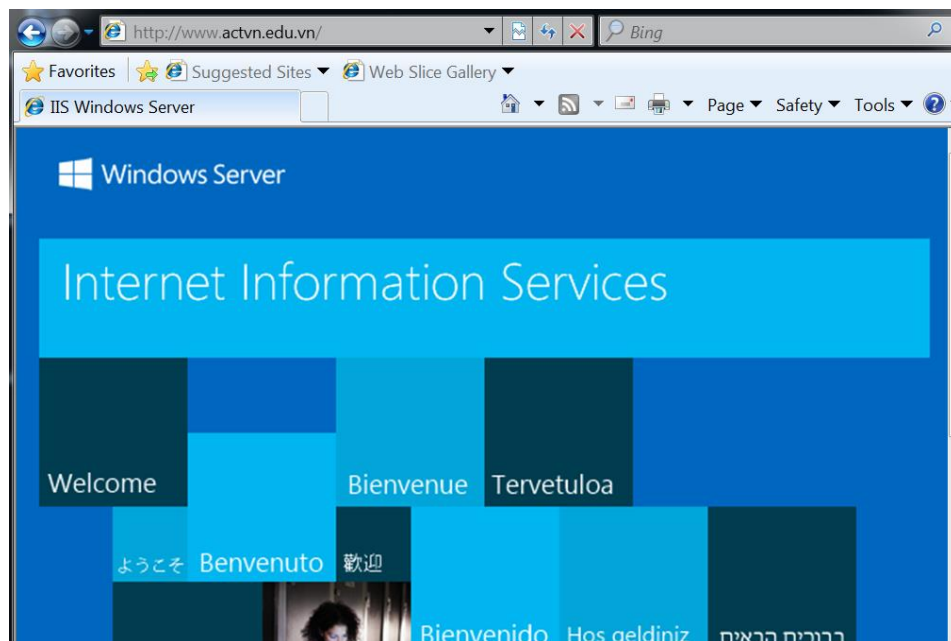
Pinging www.actvn.edu.vn [10.0.0.20] with 32 bytes of data:
Reply from 10.0.0.20: bytes=32 time=2ms TTL=127
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
```

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@server]# iptables -A FORWARD -i eth2 -o eth3 -s 172.16.1.0/24 -p tcp --dport 80 -j ACCEPT
[root@server]# iptables -A FORWARD -i eth3 -o eth2 -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:192.168.190.4
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 eth1 (kết nối Internet) trên Iptables. Kết quả không truy cập được.



Can't reach this page

- Make sure the web address <http://192.168.190.4/> is correct
- [Search for this site on Bing](#)
- [Refresh the page](#)

[More information](#)

[Fix connection problems](#)

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

Luật NAT:

```

[root@server]# iptables -t nat -A PREROUTING -i eth1 -d 192.168.190.4 -p tcp --dport 80 -j DNAT --to-destination 10.0.0.20:80

```

Luật lọc filter:

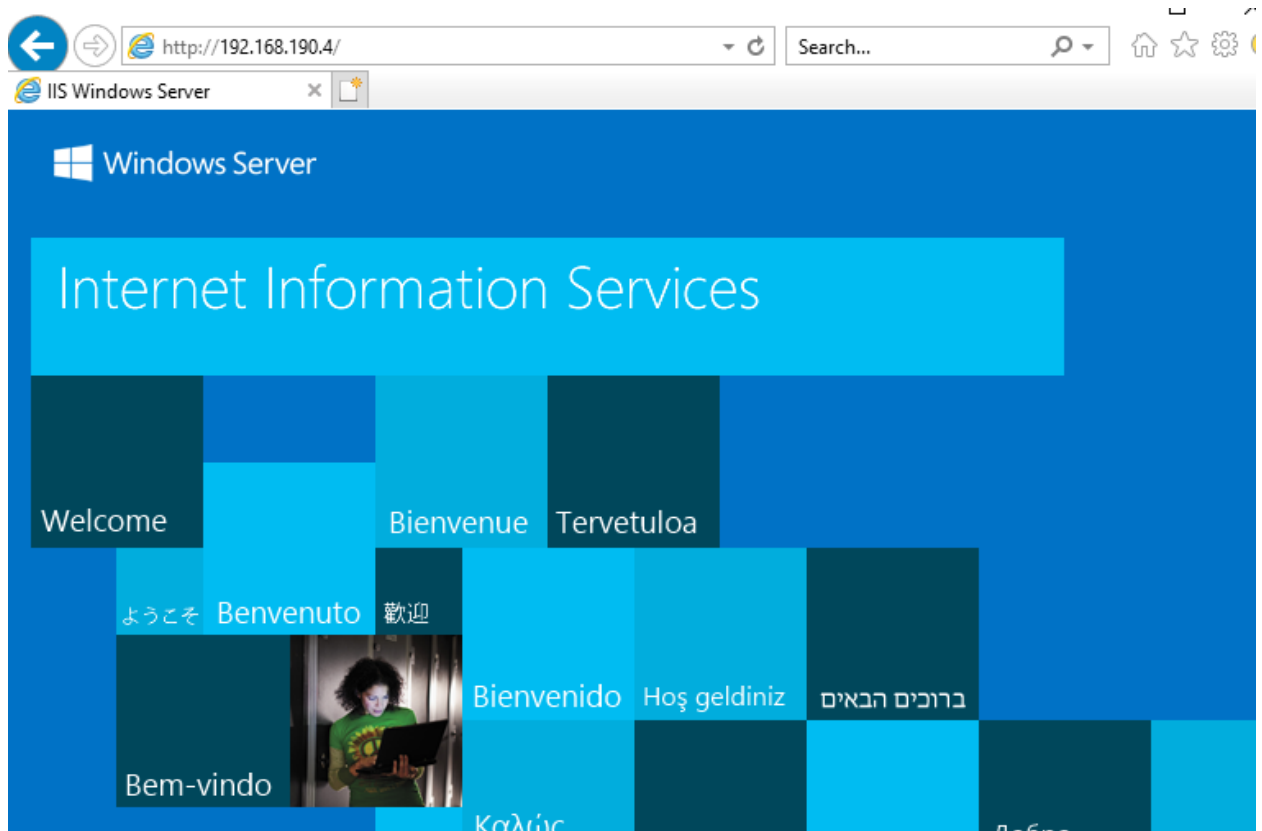
```

[root@server]# iptables -A FORWARD -i eth1 -o eth3 -d 10.0.0.20 -p tcp --dport 80 -j ACCEPT
[root@server]# iptables -A FORWARD -i eth3 -o eth1 -s 10.0.0.20 -p tcp --sport 80 -j ACCEPT

```


Bước 4. Kết quả

Từ máy vật lý, sử dụng trình duyệt web truy cập vào địa chỉ IP của giao diện mạng eth1 (kết nối Internet) trên Iptables. Kết quả thành công.

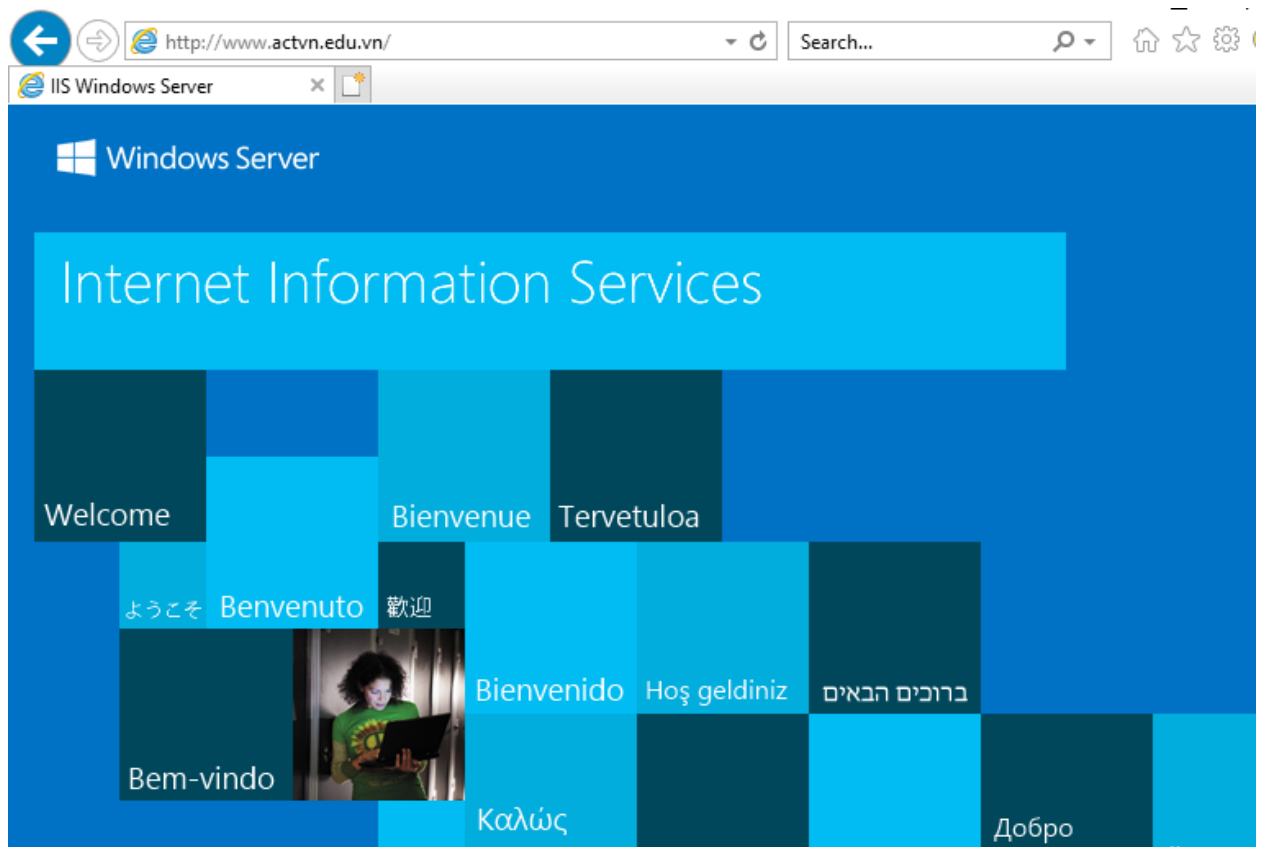


Bước 5. Để người dùng có thể truy cập được qua tên miền.

Chỉnh sửa tệp tin theo đường dẫn: C:\Windows\System32\drivers\etc\host với nội dung như sau:

```
# localhost name resolution is handled within DNS itself.
# 127.0.0.1      localhost
# ::1           localhost
192.168.190.4   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         192.168.190.4      tcp dpt:80 to:10.0.0.20:80

```

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

Mô tả:

Trong bài này cần thực hiện cấu hình tường lửa Iptables sao cho người dùng ở ngoài mạng Internet và bên trong mạng nội bộ LAN có thể gửi thư được cho nhau. Trong đó máy chủ thư được cài đặt trên máy chủ Windows Server 2012.

Bước 1. Chuẩn bị

- Máy chủ Windows Server cài đặt máy chủ thư cấu hình các bản ghi thích hợp trong dịch vụ DNS.
- Cài đặt máy chủ mail MDAemon V10 trên Windows Server và tạo các tài khoản User1, User2.

- Cài đặt phần mềm thư Thunderbird tại máy chủ vật lý và máy Windows 7.

Bước 2. Cấu hình trên máy Windows 7

Cấu hình phân giải tên miền trong file Hosts:

```
# 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
```

Kiểm tra phân giải tên miền đối với dịch vụ mail:

```
C:\Users\admin>ping mail.actvn.edu.vn

Pinging mail.actvn.edu.vn [10.0.0.20] with 32 bytes of data:
Reply from 10.0.0.20: bytes=32 time=4ms 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
Reply from 10.0.0.20: bytes=32 time=1ms TTL=127
```

Phân giải thành công.

Bật ứng dụng thư Thunderbird cấu hình như sau:

Chú ý chưa nhấn Re-test vì tường lửa chưa mở luật.

Cấu hình luật tường lửa Iptables cho phép ứng dụng mail trên máy trạm gửi và nhận thư:

```
[root@server]#iptables -A FORWARD -i eth2 -o eth3 -s
172.16.1.0/24 -p tcp -m multiport --dport 25,110 -j ACCEPT
[root@server]#iptables -A FORWARD -i eth3 -o eth2 -d
172.16.1.0/24 -p tcp -m multiport --sport 25,110 -j ACCEPT
```

Tại ứng dụng thư nhận nhấn Re-test để kết nối với máy chủ mail:

The screenshot shows a mail client configuration window. At the top, there are fields for 'Your name' (user1), 'Email address' (user1@actvn.edu.vn), and 'Password' (masked with dots). A 'Remember password' checkbox is checked. Below this, a message states: 'The following settings were found by probing the given server'. A table-like structure displays the detected settings:

	Server hostname	Port	SSL	Authentication
Incoming: POP3	mail.actvn.edu.vn	110	None	Normal password
Outgoing: SMTP	mail.actvn.edu.vn	25	None	Encrypted password

Below the table, there are fields for 'Username: Incoming:' (user1) and 'Outgoing:' (user1). At the bottom, there are buttons: 'Get a new account', 'Advanced config', 'Re-test' (highlighted in blue), 'Done', and 'Cancel'.

Kết quả thành công. Nhấn Done để kết thúc.

Bước 3. Cấu hình trên máy Vật lý

Máy vật lý cấu hình tương tự như với Windows 7:

- File Hosts:

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
192.168.190.4   www.actvn.edu.vn
192.168.190.4   mail.actvn.edu.vn
```

- Ứng dụng mail Thunderbird:

Mail Account Setup

Your name: Your name, as shown to others

Email address:

Password:

☒ Remember password

	Server hostname	Port	SSL	Authentication
Incoming: POP3	<input type="text" value="mail.actvn.edu.vn"/>	<input type="text" value="110"/>	<input type="text" value="Autodetect"/>	<input type="text" value="Autodetect"/>
Outgoing: SMTP	<input type="text" value="mail.actvn.edu.vn"/>	<input type="text" value="25"/>	<input type="text" value="Autodetect"/>	<input type="text" value="Autodetect"/>
Username: Incoming:	<input type="text" value="user2"/>		Outgoing:	<input type="text" value="user2"/>

[Get a new account](#)
[Advanced config](#)
[Re-test](#)
[Done](#)
[Cancel](#)

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

Luật NAT:

```
#iptables -t nat -A PREROUTING -i eth1 -d 192.168.190.4 -p tcp -
-dport 110 -j DNAT --to-destination 10.0.0.20:110
#iptables -t nat -A PREROUTING -i eth1 -d 192.168.190.4 -p tcp -
-dport 25 -j DNAT --to-destination 10.0.0.20:25
```

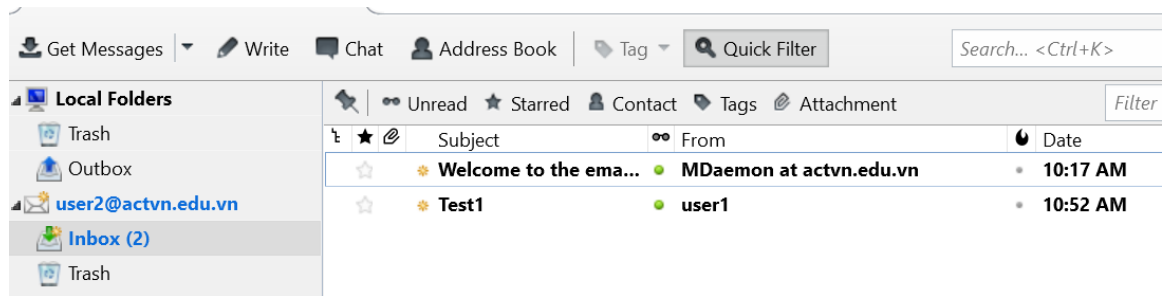
Luật lọc Filter:

```
#iptables -A FORWARD -i eth1 -o eth3 -d 10.0.0.20 -p tcp -m
multiport --dport 25,110 -j ACCEPT
#iptables -A FORWARD -i eth3 -o eth1 -s 10.0.0.20 -p tcp -m
multiport --sport 25,110 -j ACCEPT
```

Tại ứng dụng mail Thunderbird nhấn Re-test kiểm tra kết quả:

Gửi mail thành công.

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.

Tạo luật tường lửa Iptables thành công cho người dùng gửi và nhận thư.

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.

Kết thúc bài thực hành./.