ÁP DỤNG IPTABLES VÀO WEB SERVER VÀ FTP SERVER

Nguyễn Hồng Thái < *nhthai2005@gmail.com* >
Dept. of Telecommunication
Hô Chi Minh City University of Technology, South Vietnam

1. Cài đặt và cấu hình Web Server

1.1. Cài đặt Web Server

1.1.1. Web là một nhu cầu không thể thiếu hiện nay. Nó là một trong những phương tiện để mọi người trên thế giới có thể trao đổi thông tin. Đứng về phương diện nào đó thì Web có thể xem như một tờ báo điện tử, nó chứa đựng các thông tin để mọi người có thể nắm bắt một cách dễ dàng. Nó có ưu điểm hơn báo chí bình thường thông tin chứa đựng trên đó nhiều hơn, hình ảnh đặc sắc hơn…Nó còn cho phép người xem có thể tương tác phản hồi…và đặc biệt nó tiện lợi rất nhiều trong việc tìm kiếm thông tin. Nó thật sự là một công cụ không thể thiếu đối với chúng ta. Nhưng làm sao để có một trang Web? Ta cần phải có một Web Server. Web Server là nơi chứa những trang web. Web Server còn một nhiệm vụ là quản lý, bảo vệ các trang web. Và để có một Web Server thì chúng ta sẽ từng bước làm như phần trình bày dưới đây.

1.1.2. Để cài đặt Web Server thì chúng ta cần một phần mềm hỗ trợ làm điều này. Chúng ta có thể chọn *Apache*. Đây là phần mềm có nhiều tính năng mạnh và linh hoạt dùng để cài Web Server. Nó hỗ trợ đầy đủ những giao thức HTTP trước đây là HTTP/1.1. Có thể cấu hình và mở rộng với những module của công ty thứ ba. Cung cấp source code đầy đủ với license không hạn chế. Chạy trên nhiều hệ điều hành như Windows NT/9x, Netware 5.x, OS/2 và trên hầu hết các hệ điều hành Unix.

1.1.3. Đối với phiên bản Apache trên Windows, ta chỉ cần download gói về (như *apache_2.2.3-win32-x86-no-ssl.msi*) và cài đặt nó. Như vậy, chúng ta có thể sử dụng nó ngay bây giờ nếu chúng ta muốn.

1.1.4. Đối với phiên bản phiên bản trên Linux, thường thì chúng ta sẽ cài đặt ngay từ đầu lúc mà chúng ta cài đặt hệ điều hành. Còn nếu chưa cài đặt thì chúng ta có thể cài đặt nó như sau. Chúng ta có thể cài đặt từ các gói đã tạo sẵn với đuôi file thường là deb hoặc rpm, deb là các gói của Debian, dành cho các distro như: Debian, SuSe, Ubuntu … Còn rpm, đây là các gói cài đặt dành cho Red Had, viết tắt từ cụm từ RedHat Package Management. Tuy có đuôi file là như vậy nhưng chúng ta có thể cài đặt trên những distro khác ngoài nó ví dụ như các gói đuôi deb vẫn có thể cài đặt trên Red Hat hoặc các gói rpm vẫn có thể cài đặt trên Debian hay Ubuntu …, chỉ cần có trình quản lý nó. Ví dụ như với các gói đuôi rpm thì ta có trình quản lý nó là rpm còn các gói deb thì có apt-get quản lý nó. Các gói này có thể xem tương tự như trên Windows, các gói cài đặt có đuôi msi hay exe. Tuy nhiên, trên linux còn cho phép ta cài từ mã nguồn. Điều này, rất có ích cho ta chẳng hạn như có thể sửa

lại mã nguồn nếu chúng ta muốn. Lợi ích thứ 2 là chúng ta sẽ có thể quản lý được phần mềm của chúng ta. Vì trên Windows, các gói có mã nguồn là đóng vì vậy chúng ta không thể làm được điều này. Với Linux, chúng ta có thể chọn gói mã nguồn như *httpd-2.2.3.tar.gz*. Đây là gói miễn phí, chúng ta hoàn toàn có thể download được trên mạng. Và để cài đặt gói này, chúng ta sẽ làm như sau:

- Giải nén mã nguồn dùng lệnh: *tar xvzf httpd-2.2.3.tar.gz*
- Di chuyển vào thư mục chứa mã nguồn: *cd httpd-2.2.3*
- Sau đó, chúng ta sẽ lần lượt cài đặt nó:
  # ./configure && make && make install.
- Nếu cài đặt trên Debian hay Ubuntu thì gõ lệnh: *apt-get install apache*
- Còn nếu cài đặt từ những gói rpm thì gõ lệnh: *rpm -ivh httpd-2.2.3.rpm*
- Bây giờ, chúng ta có thể chạy Web Server nếu chúng ta muốn. Tuy nhiên, vẫn có khi gặp trường hợp không thể khởi động được như: lỗi vì đã có phần mềm nào đó chạy trên port mà Web Server ta sẽ chạy. Điều này có thể khắc phục được một cách dễ dàng, bằng cách tắt chương trình chạy trên port đó đi. Và bây giờ khởi động lại là có thể chạy được.
- Để khởi động hay tạm dừng hay tái khởi động apache ta script sau:
  # /etc/init.d/httpd start/stop/restart
  Hoặc dùng lệnh:
  #chkconfig httpd on
  #service httpd restart
- Tuy nhiên, để có thể hiểu cũng như có thể vận hành theo đúng ý muốn của chúng ta thì ta cần phải hiểu và cũng như phải tận tay cấu hình nó. Và việc cấu hình đó, chúng tôi sẽ trình bày trong mục 2 phần cấu hình Web Server dưới đây.

1.2. Cấu hình Web Server

Các tập tin và thư mục cấu của Apache:

- **/etc/httpd/conf**: thư mục lưu giữ các tập tin cấu hình như *httpd.conf.*
- **/etc/httpd/modules**: lưu giữ các module của Web Server.
- **/etc/httpd/logs:** lưu các tập tin log của Apache.
- **/var/www/html:** lưu các trang web.
- **/var/www/cgi-bin:** lưu các script sử dụng cho các trang web.

Tập tin cấu hình Apache được tạo thành từ nhiều chỉ dẫn (directive) khác nhau. Mỗi dòng hoặc mỗi một directive và phục vụ cho một cấu hình riêng biệt. Có những directive có ảnh hưởng với nhau. Những dòng bắt đầu bằng dấu # là những dòng chú thích. Sau đây là những directive quan trọng khi cấu hình Web Server.

- **ServerName:**

Cú pháp: ServerName <hostname>:port

Trong đó, hostname là tên máy tính của Server. Nó được dùng trong việc tạo ra những URL chuyển tiếp (direction URL). Nếu không chỉ ra, server sẽ cố gắng suy luận từ địa chỉ IP của nó. Tuy nhiên, điều này có thể không tin cậy hoặc không trả ra tên máy tính đúng.

Ví dụ: ServerName www.nguyenhongthai.hcmut.edu.vn

- **ServerAdmin:** địa chỉ email của người quản trị hệ thống
  Cú pháp: ServerAdmin <địa chỉ email>
  Ví dụ: ServerAdmin webmaster@hcmut.edu.vn

- **ServerType:** quy định cách nạp chương trình. Có 2 cách:
  inetd: chạy từ các init level.
  standalone: chạy từ hệ thống.
  Cú pháp: ServerType <inetd/standalone>
  Ví dụ: ServerType standalone

- **DocumentRoot:** cấu hình thư mục gối lưu trữ nội dung của Website. Web Server sẽ lấy những tập tin trong thư mục này phục vụ cho yêu cầu của client
  Cú pháp: DocumentRoot <đường dẫn thư mục>
  Ví dụ: DocumentRoot/usr/web

- **ServerRoot:** chỉ dẫn vị trí cài đặt chương trình Apache.
  Cú pháp: ServerRoot <vị trí cài đặt Apache>
  Ví dụ: ServerRoot /user/local/apache

- **ErrorLog:** chỉ ra tập tin để server ghi vào bất kỳ những lỗi nào mà nó gặp phải.
  Cú pháp: ErrorLog <vị trí tập tin log>
  Ví dụ: ErrorLog logs/error_log

- **DirectoryIndex**: các tập tin mặc định được truy vấn khi truy cập trang Web.
  Cú pháp: DirectoryIndex <danh sách các tập tin>
  Ví dụ: DirectoryIndex index.html

- **MaxClients:** quy định số yêu cầu tối đa từ các client có thể gởi đồng thời đến server.
  Cú pháp: MaxClients <số kết nối tối đa cho phép>
  Ví dụ: MaxClients 256

- **Listen:** quy định địa chỉ IP hoặc cổng mà Apache nhận kết nối từ Client.
  Cú pháp: Listen <Port/IP>
  Ví dụ: Listen 80

- **BindAddress**: quy định địa chỉ card mạng để chạy Apache trên Server.
  Cú pháp: BindAddress <IP/*>
  Sử dụng dấu "*" để có thể sử dụng tất cả các địa chỉ trên máy.
  Ví dụ: BindAddress 172.28.24.199

- **TimeOut:** quy định thời gian sống của một kết nối (được tính bằng giây).
  Cú pháp: TimeOut <thời gian tối đa cho một kết nối>
  Ví dụ: TimeOut 300

- **KeepAlive:** cho phép hoặc không cho phép client gửi được nhiều yêu cầu dựa trên một kết nối đến với Web Server.
  Cú pháp: KeepAlive <On/Off>

Ví dụ: KeepAlive On

- **MaxKeepAliveRequests:** số Request tối đa trên một kết nối (nếu cho phép nhiều Request trên một kết nối).

Cú pháp: MaxKeepAliveRequests <số Request>
Ví dụ: MaxKeepAliveRequests 100

- **KeepAliveTimeout:** quy định thời gian để chờ một Request kế tiếp từ cùng một client trên cùng một kết nối (được tính bằng giây).

Cú pháp: KeepAliveTimeout <thời gian>
Ví dụ: KeepAliveTimeout 15

- **Alias:** ánh xạ đường dẫn cục bộ (không nằm trong DocumentRoot) thành tên đường dẫn địa chỉ URL.

Cú pháp: Alias <đường dẫn http><đường dẫn cục bộ>
Ví dụ: Alias /doc /usr/share/doc
Khi truy cập *http://www.nguyenhongthai.hcmut.edu.vn/doc*, nó sẽ vào /usr/share/doc. Để giới hạn việc truy cập của người dùng ta có thể kết hợp với Directory directive.
Ví dụ:

```
Alias /doc /usr/share/doc
<Directory /usr/share/doc>
        AuthType Basic          # kiểu authentication sẽ sử dụng là Basic
        AuthName intranet       # đặt tên cho sự chứng thực là intranet
        AuthUserFile /etc/httpd/passwd      # vị trí của tập tin password
        Require user hongthai minhtri #user cho phép truy cập tài nguyên
        Allow from internal.hcmut.edu.vn # cho phép truy cập từ đchỉ này
</Directory>
```

- **UserDir:** cho phép người dùng tạo Home page của user trên Web Server.

Cú pháp:

```
<IfModule mod_userdir.c>
#UserDir Disables      ## để thực thi cơ chế enable UserDir
UserDir www  ## Khai báo thư mục chứa Website của user
</IfModule>
<Directory /home/*/www>
        ...
</Directory>
```

Trong thư mục Home Directory của người dùng tạo thư mục www. Ví dụ /home/nhthai/www. Khi đó, cú pháp truy cập từ Web Browser có dạng: *http://www.nguyenhongthai.hcmut.edu.vn/~<tênUser>*, tức trong trường hợp này là *http://www.nguyenhongthai.hcmut.edu.vn/~nhthai*. Khi người dùng có gắng truy cập đến thư mục của mình, có thể gặp một message lỗi "Forbidden". Điều này có thể là quyền truy cập đến home directory của người dùng bị giới hạn. Như vậy để khắc phục lỗi trên, chúng ta cần giới hạn lại quyền truy cập home directory của người dùng với những câu lệnh như sau:

```
chown nhthai /home/nhthai /home/nhthai/www
chmod 750    /home/nhthai /home/nhthai/www
```

- **VirtualHost:** là tính năng của Apache, giúp ta duy trì nhiều hơn một web server trên một máy tính. Nhiều tên cùng chia sẻ một địa chỉ IP gọi là named-based virtual hosting và sử dụng những địa chỉ IP khác nhau cho từng domain gọi là IP-based virtual hosting.

  - **IP-based Virtual Host:** Virtual Host dựa trên IP yêu cầu những server phải có một địa chỉ IP khác nhau cho mỗi virtual host dựa trên IP. Như vậy, một máy tính phải có nhiều interface hay sử dụng cơ chế virtual interface mà những hệ điều hành sau hỗi trợ. Nếu máy của chúng ta có một địa chỉ IP, 172.28.24.199, chúng ta có thể cấu hình một địa chỉ IP khác trên cùng một card mạng như sau:

```
ifconfig eth0:1 172.28.24.198 netmask 255.255.255.0 up
```

Sau đó, chúng ta mô tả thông tin cấu hình trong file httpd.conf

```
<VirtualHost *> ; VirtualHost default
    ...
    DocumentRoot/tmp
    ServerName          www.domain
    ...
</VirtualHost>
<VirtualHost 172.28.24.199>;VirtualHost cho site 1
    ...
    DocumentRoot/home/www/site1
    ServerName          www1.domain
</VirtualHost>
<VirtualHost 172.28.24.198>;VirtualHost cho site 2
    ...
    DocumentRoot/home/www/site2
    ServerName          www2.domain
    ...
</VirtualHost>
```

  - **Name-based Virtual Host:** IP-based Virtual Hosts dựa vào địa chỉ IP để quyết định *Virtual Host* nào đúng để truy cập. Vì thế, chúng ta cần phải có địa chỉ khác nhau cho mỗi *Virtual Host*. Với Named-based Virtual Host, server dựa vào HTTP header của client để biết được hostname. Sử dụng kỹ thuật này, một địa chỉ IP có thể có nhiều tên máy tính khác nhau. Named-based Virtual Host rất đơn giản, chúng ta chỉ cần cấu hình DNS sao cho nó phân giải mỗi tên máy đúng với một địa chỉ IP và sau đó cấu hình Apache để tổ chức những web server cho những miền khác nhau.

2. Cài đặt và cấu hình FTP Server

2.1.Cài đặt FTP Server

- Cũng như Web, FTP cũng là một công cụ không thể thiếu trong lĩnh vực mạng. FTP là chữ viết tắt của File Transfer Protocol. Giao thức này được xây dựng dựa trên chuẩn TCP. FTP cung cấp cơ chế truyền tin dưới dạng file thông qua mạng TCP/IP. FTP là dịch vụ đặc biệt vì nó dùng đến 2 cổng: cổng 20 dùng để truyền dữ liệu (data port) và

cổng 21 dùng để truyền lệnh (command port). FTP hoạt động ở một trong 2 cơ chế: cơ chế chủ động (active) và cơ chế bị động (passive).

- Khi FTP Server hoạt động ở cơ chế chủ động, client không chủ động tạo kết nối thật sự vào cổng dữ liệu của FTP Server, mà chỉ đơn giản là thông báo cho server biết rằng nó đang lắng nghe trên cổng nào và server phải kết nối ngược về client vào cổng đó. Trên quan điểm firewall đối với máy client điều này giống như một hệ thống bên ngoài khởi tạo kết nối vào hệ thống bên trong và điều này thường bị ngăn chặn trên hầu hết hệ thống firewall.
- Để giải quyết vấn đề server phải tạo kết nối đến client, một phương thức kết nối FTP khác đã được phát triển. Phương thức này gọi là FTP thụ động hoặc PASV (là lệnh mà client gởi cho server để báo cho biết nó đang ở chế độ passive). Trong khi FTP ở chế độ thụ động giải quyết được vấn đề phía client thì nó gây ra nhiều vấn đề khác về phía server. Thứ nhất là cho phép máy ở xa kết nối vào cổng bất kỳ lớn hơn 1024 của server. Điều này khá nguy hiểm trừ khi FTP cho phép mô tả dãy các cổng lớn hơn hoặc bằng 1024 mà FTP sẽ dùng. Vấn đề thứ hai là, một số FTP client lại không hỗ trợ chế độ thụ động. Ví dụ tiện ích FTP mà Solaris cung cấp không hỗ trợ FTP thụ động. Khi đó, cần phải dùng thêm trình FTP client. Một lưu ý khác là hầu hết các trình duyệt Web chỉ hỗ trợ FTP thụ động khi truy cập FTP server theo đường URL ftp://.
- Chương trình FTP Server: FTP Server là một máy chủ lưu giữ những tài nguyên và hỗ trợ giao thức FTP để giao tiếp với những máy tính khác. Nó cho phép truyền dữ liệu trên Internet. Một số chương trình FTP Server sử dụng trên Linux như: vsftpd, Wu-ftpd, PureFTPd, ProFTPD Trên Windows, ta có thể sử dụng phiên bản hỗ trợ của MicroSoft hoặc có thể sử dụng phiên bản của Golden như: *Golden-FTP-server-PRO-setup.exe (bản đòi hỏi license)* hoặc có thể dùng bản miễn phí *GoldenFTPserver-setup.exe.*
- Về phần cài đặt, nếu cài trên Windows sử dụng phiên bản hỗ trợ của MicroSoft, ta vào *Control Panel → Add/Remove Program → Add/Remove Windows Components → Chọn IIS → Chọn install*. Còn dùng phiên bản của Golden thì ta chỉ cài gói cài đặt trên duy nhất.
- Bây giờ, chúng tôi sẽ trình bày phần cài đặt từ source cho linux. Chọn gói cài đặt là *vsftpd-2.0.5.tar.gz*. Các bước sẽ tiến hành như sau:

```
# tar xvzf vsftpd-2.0.5.tar.gz  ## Giải nén mã nguồn
# cd vsftpd-2.0.5               ## Di chuyển đến thư mục chứa mã nguồn
# make                          ## Tạo binary file
# make /var/ftp                 ## Tạo thư mục chứa các file để truy cập FTP
# useradd -d /var/ftp ftp       ## Tạo tài khoản người dùng vào thư mục chỉ định
# chown root.root /var/ftp      ## Chuyển quyền sở hữu sang root
# chmod go-w /var/ftp           ## Không cho phép ghi đối với người dùng khác
# make install                  ## Cài đặt FTP Server
```

Nếu không thực hiện được lênh 'make install' thì ta có thể làm như sau:

```
# cp vsftpd /usr/local/sbin/vsftpd
# cp vsftpd.conf.5 /usr/local/man/man5
# cp vsftpd.8 /usr/local/man/man8
```

Tiếp theo, là chép file cấu hình vào thư mục /etc:
cp vsftpd.conf /etc
Cuối cùng, ta cần chỉnh sửa một chút để cho phép làm việc theo kiểu nào. Nếu cho chạy theo kiểu *standalone* thì thêm dòng *listen=YES* vào cuối file */etc/vsftpd.conf.* Còn nếu muốn cho chạy vơi inetd thì thêm dòng
ftp stream tcp nowait root /usr/sbin/tcpd /usr/local/sbin/vsftpd vào file */etc/inetd.conf.*

❖ Nếu không quen với việc cài đặt từ mã nguồn, ta có thể chọn các cài cài đặt đã làm sẵn như những gói có đuôi deb hoặc rpm. Và việc cài đặt các gói này tương tự như cài đặt Web Server.

❖ Vsfpd là một package mới. Nó được phát triển xoay quanh tính năng nhanh, ổn định và an toàn. Vsftpd có khả năng quản lý số lượng kết nối lớn một cách hiệu quả và an toàn.

Để khởi động và dừng vsftpd:
service vsftpd start/stop/restart
Hoặc sử dụng lệnh:
/etc/init.d/vsftpd start/stop/restart

2.2.Cấu hình FTP Server

Những tập tin và thư mục thường được qua tâm khi cấu hình vsftpd server:

- **/etc/pam.d/vsftpd**: tập tin cấu mục PAM cho vsftpd. Tập tin này định nghĩa những yêu cầu mà người dùng phải cung cấp khi đăng nhập vào ftp server.

PAM là chữ viết tắt từ Pluggable Authentication Modules, tạm dịch là các mô-đun kiểm tra có thể cắm được. PAM được phát triển cho hệ thống Solaris từ Sun MicroSystems. Dự án Linux-PAM làm cho PAM có sẵn đối với hệ điều hành Linux. PAM là bộ thư viện dùng chung để cấp phát các đặc quyền cho ứng dụng liên quan đến PAM.

- **/etc/vsftpd/vsftpd.conf**: tập tin cấu hình vsftpd server.
- **/etc/vsftpd.ftpusers**: liệt kê những người dùng không được login vào vsftpd. Mặc định, danh sách những người dùng này gồm root, bin, deamon và những người dùng khác.
- **/etc/vsftpd.user_list**: tập tin này được cấu hình để cấm hay cho phép những dùng được liệt kê truy cập ftp server. Điều này phụ thuộc vào tùy chọn userlist_deny được xét *YES hay NO* trong tập tin *vsftpd.conf*. Nếu những người dùng đã liệt kê trong tập tin này thì không được xuất hiện trong *vsftpd.ftpusers*.
- **/var/ftp:** thư mục chứa các tập tin đáp ứng cho vsftpd. Nó cũng chứa thư mục pub cho người dùng *anonymous* (có thể hiểu là người dùng ẩn danh). Thư mục này chỉ có thể đọc, chỉ có root mới có khả năng ghi.

3. Cấu hình để LAN có thể truy cập mạng bên ngoài

Việc cấu hình để các máy từ LAN có thể truy cập ra bên ngoài internet. Đây là mô hình cho phép nhiều máy cùng chia sẽ một IP public. Để có thể làm điều này trên hệ điều hành Linux, ta có thể chọn lựa tool chạy rất ổn định, đó là iptables để cấu hình. Ngoài mục đích trên, iptables còn có thể dùng để lọc gói tin rất hiệu quả. Chúng ta có thể cho phép những gói tin nào đó hay chặn những gói tin nào đó mà ta muốn. Để thực hiện một cách cụ thể, chúng tôi đưa ra một mô hình cụ thể tự chúng tôi thiết lập và đã cho chạy thực tế. Sử

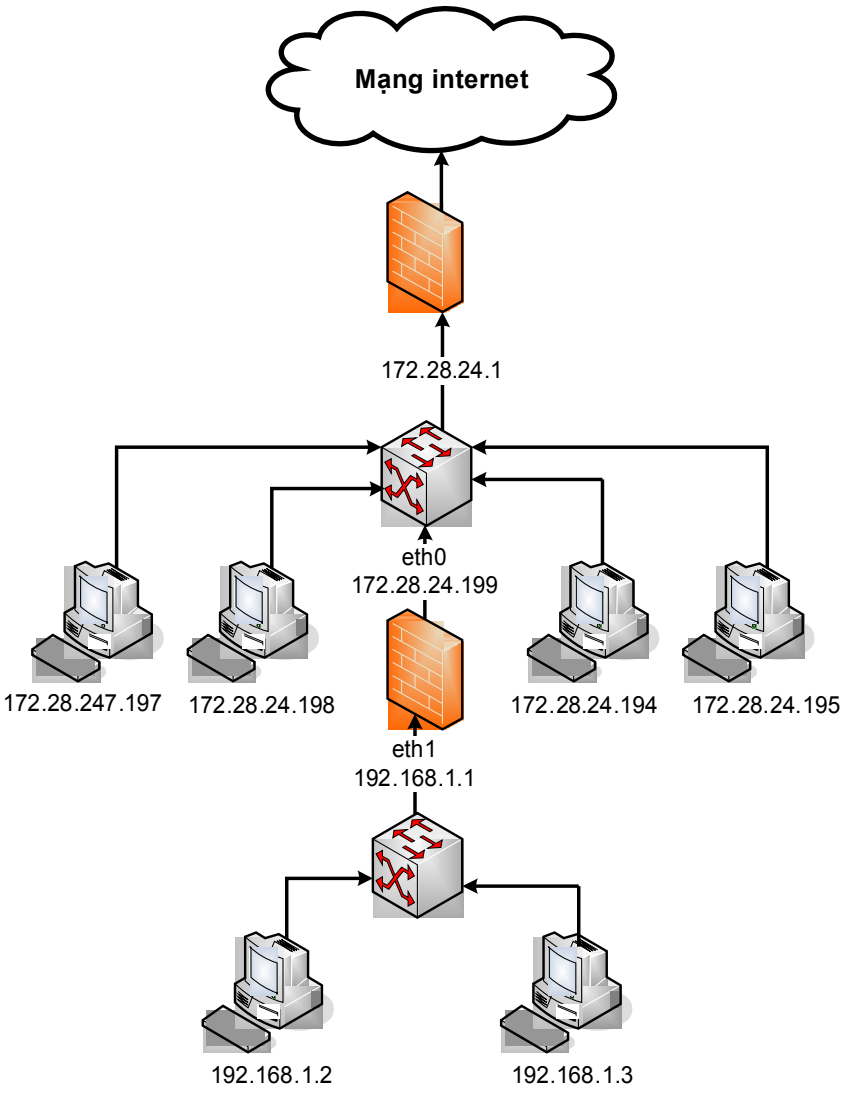
dụng mạng máy tính cụ thể, đó là mạng máy tính của phòng máy tính khoa điện - điện tử. Với mô hình thiết lập như hình dưới đây.

Việc cấu hình có thể được giải thích như sau. Để một gói tin đi từ một mạng LAN bên trong ra mạng bên ngoài thì ta cần phải thay đổi địa chỉ nguồn của gói tin để khi ra khỏi mạng LAN mà muốn định tuyến được thì mạng đó đòi hỏi phải cùng subnet và đồng thời đòi hỏi địa chỉ nguồn phải được đổi trước khi nó thực hiện định tuyến ra ngoài. Do đó, ta thực hiện Source NAT. Và cứ như thế nó sẽ có thể đi ra ngoài mạng internet. Và việc cấu hình Source ta có thể chọn iptables. Chúng tôi sẽ trình bày việc cấu hình SNAT tại máy dùng làm gateway của mạng 192.168.1.0/24. Trình tự các bước sẽ làm như sau:

```
# modprobe ipt_MASQUERADE   ## Load mô-đun ip_MASQUERADE
# iptables -F               ## Xóa các luật trong bảng filter
# iptables -t nat    -F     ## Xóa các luật trong bảng nat
# iptables -t mangle -F     ## Xóa các luật trong bảng mangle
## Nếu gói tin đi từ 192.168.1.0/24 ra mạng ngoài thì thực hiện đổi địa chỉ
##### nguồn thành 172.28.24.199
# iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 172.28.24.199
## Cho phép các interface có thể forward được với nhau
# echo 1 > /proc/sys/net/ipv4/ip_forward
## Cho phép các gói tin từ các kết nối đã thiết lập hoặc có mối liên hệ với
### kết nối hiện tại. Lệnh này có ý nghĩa trong trường hợp kết nối FTP
# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
## Cho phép các gói tin đến từ những interface không phải eth0
# iptables -A INPUT -m state --state NEW -i ! eth0 -j ACCEPT
## Mặc định là DROP (cấm)
# iptables -P INPUT DROP
## Nếu gói tin forward từ eth0 đến eth0 thì ngăn lại và trả thông báo về
### cho người gởi biết
# iptables -A FORWARD -i eth0 -o eth0 -j REJECT
```

Trong trường hợp đường nối ra mạng ngoài không phải là card ethernet mà là dial up thì ta sẽ đổi *eth0* thành *ppp0*

Với việc cấu hình iptables trên trong trường hợp mô hình mạng như hình 7.1.Giả máy 192.168.1.2 muốn gởi Request đến máy 172.28.2.2. Suy ra, gói tin sẽ có địa chỉ nguồn là 192.168.1.2 và địa chỉ đích là 172.28.2.2. Nó sẽ định tuyến đến gateway vì địa chỉ đích không cùng subnet của địa chỉ nguồn, tại đây iptables sẽ thiết lập lại gói tin, tức sẽ đổi địa chỉ nguồn thành 172.28.24.199 còn địa chỉ đích giữ nguyên. Tiếp theo, nó mới thực hiện định tuyến. Và việc định tuyến sẽ giống như trên, nó xem lại gói tin rõ ràng địa chỉ đích không cùng subnet của địa chỉ nguồn, nó sẽ định tuyến đến gateway và sẽ thực hiện đổi địa chỉ nguồn tại đây. Việc định tuyến cứ tiếp tục như thế. Đến khi nó thấy rằng gói tin có địa chỉ đích có cùng subnet với địa chỉ nguồn thì nó xác định được máy cần đến nằm tại mạng này. Và như thế, nó sẽ không cần đến gateway mà chỉ cần đến switch và chuyển gói tin thẳng đến đích. Quá trình trình gởi Reponse từ máy 172.28.2.2 về máy 192.168.1.2, nó sẽ xem header mà định tuyến về đích.



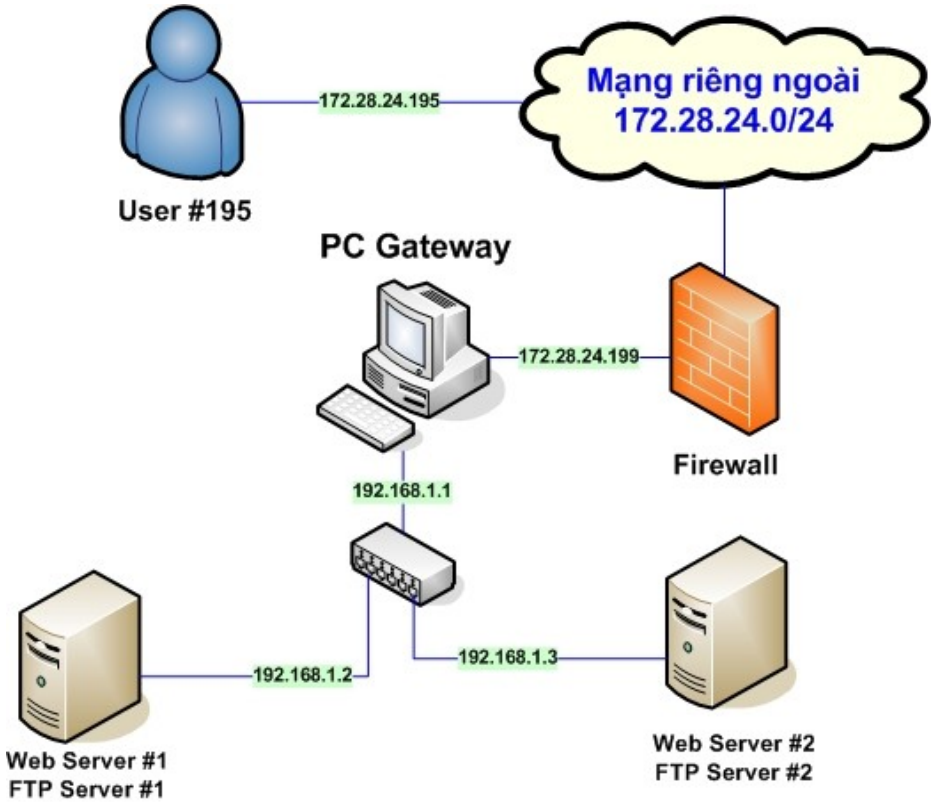
Hình 1: Mô hình mạng LAN tự thiết lập

4. Cấu hình để mạng bên ngoài có thể truy cập được các Server

Việc cấu hình để mạng bên ngoài có thể truy cập được các Server từ một LAN nội bộ. Đây cũng là mô hình rất phổ biến. Nó có thể làm công việc cân bằng tải vừa tạo tính an toàn cho mạng nội bộ. Phương pháp thực hiện điều này có thể lý giải ngắn gọn như sau: người dùng internet muốn truy cập đến một trang web nào đó thì trên URL họ chỉ gõ địa chỉ của Server ảo (hay còn gọi là VIP, viết tắt từ cụm từ Virtual IP). Và Server ảo này cũng là gateway, tại đây ta cũng thiết lập tường lửa. Tại đây, nó sẽ xem xét địa chỉ cũng như port, sau đó nó sẽ forward đến server cần thiết Mô hình cấu hình server do chúng tôi tự thiết lập được minh họa ở hình dưới đây. Và trình tự cấu hình sẽ lần lượt như sau:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward ## Cho phép IP forwarding
## Load các modules
# modprobe ip_conntrack_ftp
```

```
# modprobe ip_nat_ftp
##Thiết lập các chính sách mặc định và giải phóng các bảng của iptables
# iptables -t nat -F
# iptables -P INPUT ACCEPT
# iptables -F INPUT
# iptables -P OUTPUT ACCEPT
# iptables -F OUTPUT
# iptables -P FORWARD ACCEPT
# iptables -F FORWARD
## Cấu hình Web Server trên máy 192.168.1.2
## Đổi địa chỉ đích của gói tin khi gói tin có địa chỉ đích là 172.28.24.199
## port 80, đi vào eth0, dùng giao thức tcp thành 192.168.1.2 port 8080
# iptables -t nat -A PREROUTING -d 172.28.24.199 -i eth0 -p tcp \
--dport 80 -j DNAT --to-destination 192.168.1.2:8080
# Cho phép các gói tin trên có thể forward
# iptables -A FORWARD -p tcp -i eth0 -d 192.168.1.2  --dport 8080  \
-j ACCEPT
## Tương tự, ta cấu hình Web Server trên máy 192.168.1.3
# iptables -t nat -A PREROUTING -d 172.28.24.199 -i eth0 -p tcp  \
--dport 8888 -j DNAT --to-destination 192.168.1.3:80
## Cấu hình FTP Server trên máy 192.168.1.3
# iptables -A FORWARD -p tcp -i eth0 -d 192.168.1.3  --dport 80  \
-j ACCEPT
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 20:21 \
-j DNAT --to-destination 192.168.1.2:21
# iptables -A FORWARD -p tcp -i eth0 -d 192.168.1.2 --dport 21  \
-j ACCEPT
## Tương tự, ta cấu hình cho máy 192.168.1.3
# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2020:2121 \
-j DNAT --to-destination 192.168.1.3:21
# iptables -A FORWARD -p tcp -i eth0 -d 192.168.1.3 --dport 21  \
-j ACCEPT
```



MÔ HÌNH MẠNG LAN TỰ THIẾT LẬP

Hình 2: Mô hình mạng LAN cùng với các server

5. Kết quả của việc cấu hình trên

Kết quả của việc cấu hình iptables sẽ được lưu trong file /etc/sysconfig/iptables như sau:

```
# Generated by iptables-save v1.2.8 on Thu Nov  9 15:47:54 2006
*nat
:PREROUTING ACCEPT [4169:438355]
:POSTROUTING ACCEPT [106:6312]
:OUTPUT ACCEPT [22:1332]
-A PREROUTING -d 172.28.24.199 -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination
192.168.1.2:8080
-A PREROUTING -d 172.28.24.199 -i eth0 -p tcp -m tcp --dport 8888 -j DNAT --to-destination
192.168.1.3:80
-A PREROUTING -i eth0 -p tcp -m tcp --dport 20:21 -j  DNAT --to-destination 192.168.1.2:21
-A PREROUTING -i eth0 -p tcp -m tcp --dport 2020:2121 -j  DNAT --to-destination 192.168.1.3:21
-A POSTROUTING -o eth0 -j SNAT --to-source 172.28.24.199
COMMIT
# Completed on Thu Nov  9 15:47:54 2006
# Generated by iptables-save v1.2.8 on Thu Nov  9 15:47:54 2006
*filter
:INPUT DROP [4011:414080]
```

```
:FORWARD ACCEPT [552:57100]
:OUTPUT ACCEPT [393:43195]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i ! eth0 -m state --state NEW -j ACCEPT
-A FORWARD -d 192.168.1.3 -i eth0 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Thu Nov  9 15:47:54 2006
# Generated by iptables-save v1.2.8 on Thu Nov  9 15:47:54 2006
*mangle
:PREROUTING ACCEPT [5114:853418]
:INPUT ACCEPT [4416:773589]
:FORWARD ACCEPT [552:57100]
:OUTPUT ACCEPT [393:43195]
:POSTROUTING ACCEPT [945:100295]
COMMIT
# Completed on Thu Nov  9 15:47:54 2006
```

Kết quả khi thực hiện *traceroute* từ máy 192.168.1.2 đến máy khác như sau:

```
sysadmin@debian:~$ traceroute 172.28.24.195
traceroute to 172.28.24.195 (172.28.24.195), 30 hops max, 38 byte packets
1  192.168.1.1 (192.168.1.1)  2.541 ms  3.409 ms  0.142 ms
2  172.28.24.195 (172.28.24.195)  0.298 ms  3.125 ms  0.256 ms

sysadmin@debian:~$ traceroute 172.28.2.2
traceroute to 172.28.2.2 (172.28.2.2), 30 hops max, 38 byte packets
1  192.168.1.1 (192.168.1.1)  0.259 ms  4.546 ms  0.185 ms
2  172.28.24.1 (172.28.24.1)  1.182 ms  2.777 ms  0.820 ms
3  hcmut-server.hcmut.edu.vn (172.28.2.2)  0.988 ms  4.159 ms  5.069 ms
sysadmin@debian:~$
```

Kết quả khi thực hiện *mtr* từ máy 192.168.1.2 đến máy khác như sau:

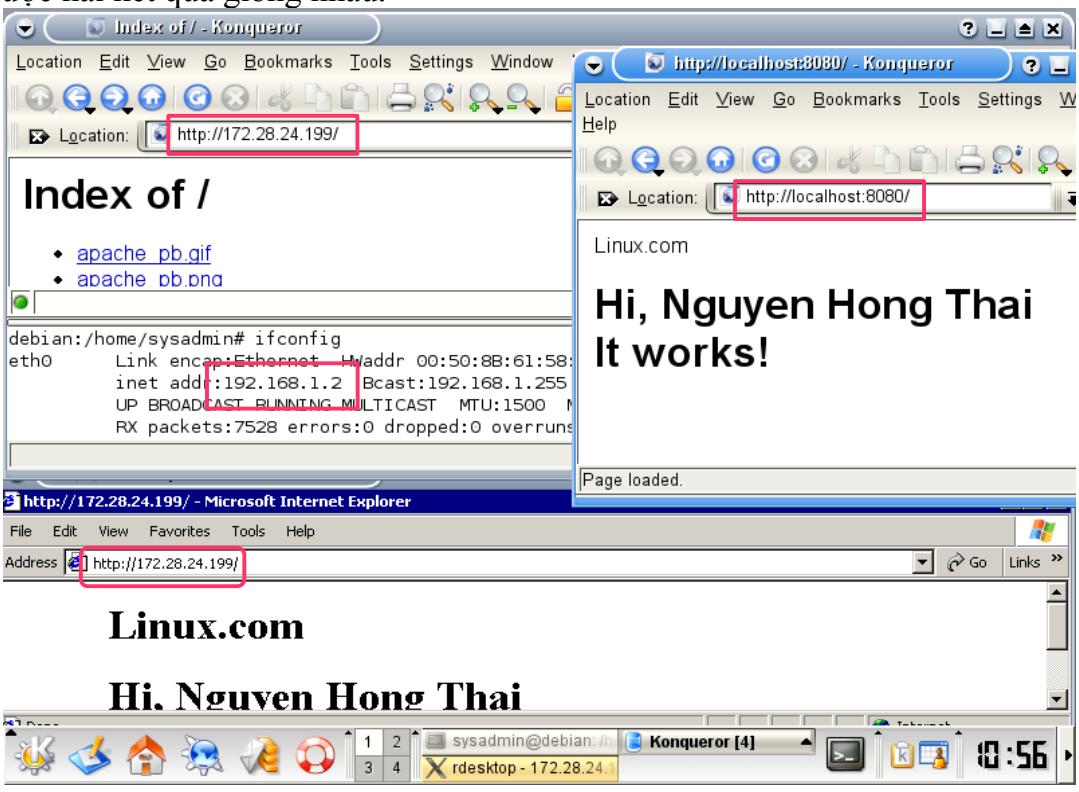
```
                    My traceroute  [v0.67]
debian (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)  Wed Nov 15 11:11:31 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
Packets                               Pings
Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 192.168.1.1                 0.0%    70    0.3   1.4   0.2  59.0   7.2
2. 172.28.24.195               0.0%    70    0.4   6.8   0.3 292.3  35.7

                    My traceroute  [v0.67]
debian (0.0.0.0)(tos=0x0 psize=64 bitpattern=0x00)  Wed Nov 15 11:13:13 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
Packets                               Pings
Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 192.168.1.1                 0.0%    12    0.2   0.3   0.2   1.2   0.3
2. 172.28.24.1                 0.0%    12    0.9   1.5   0.8   6.0   1.6
3. hcmut-server.hcmut.edu.vn   0.0%    12    0.4   0.9   0.4   4.7   1.3
```

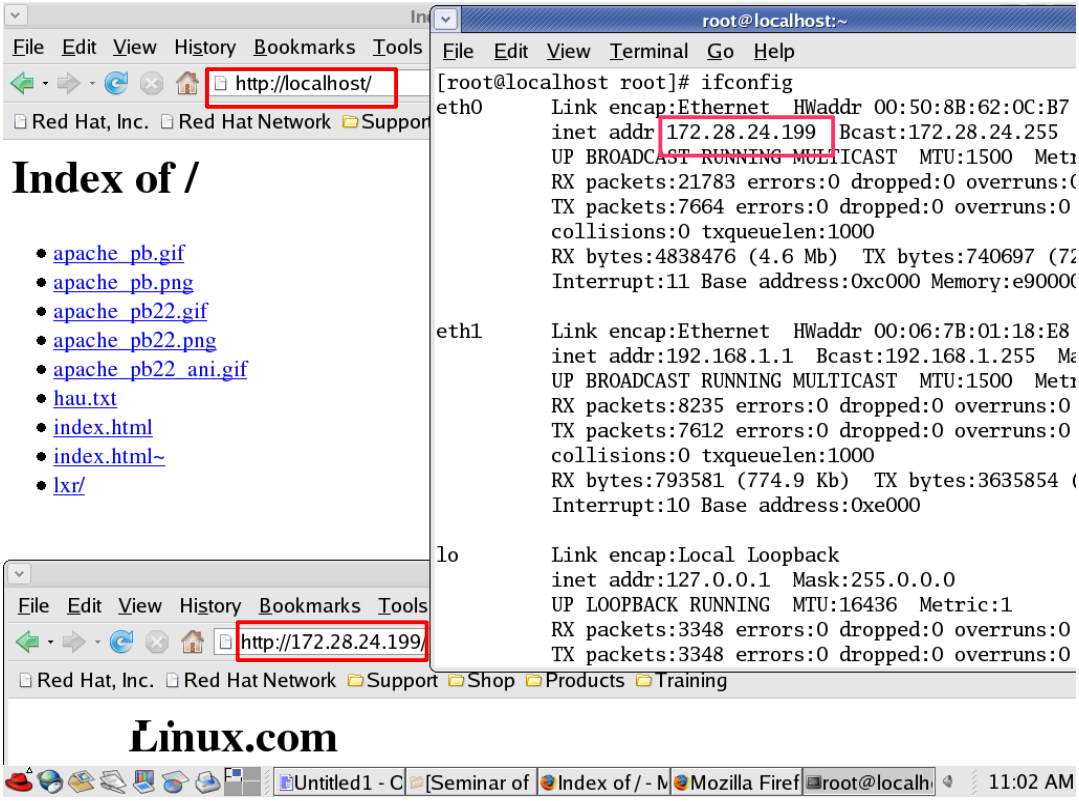
Kết quả từ máy 192.168.1.2, dùng Konqueror để truy cập Web server. Nếu ở URL gõ http://localhost:8080/ máy tính sẽ hiểu là truy cập Web Server trên máy máy 192.168.1.2 trên port 8080. Điều này có thể dễ dàng nhận ra vì dùng lệnh *ifconfig* thì thấy rằng địa chỉ 192.168.1.2 chính là địa chỉ của interface eth0 của máy 192.168.1.2. Còn nếu ở URL gõ http://172.28.24.199 thì nó sẽ hiểu địa chỉ này không phải địa chỉ trong mạng của nó. Do đó, nó gởi đến gateway và trên gateway sẽ định tuyến gói theo quy luật mà iptables đã cài ở trên (ở phần *cài đặt để LAN có thể truy cập ra mạng bên ngoài*). Nó ánh xạ địa chỉ 172.28.24.199 port 80 → 192.168.1.2 port 8080. Vì vậy, mà tuy gõ hai địa chỉ ở URL khác nhau nhưng kết quả trả về từ web server là giống nhau. Đồng thời, trên máy 192.168.1.2 ta đăng nhập từ xa đến một máy khác ngoài mạng thử dùng Internet Explorer để truy cập http://172.28.24.199 thì ta vẫn nhận được kết quả từ web server hoàn toàn giống với 2 kết quả trên.

Còn nếu trên máy dùng làm gateway ta dùng Mozilla Firefox để truy cập http://localhost/ thì nó sẽ hiểu là truy cập Web Server trên máy này mặc dù máy này có địa chỉ 172.28.24.199. Ta rõ ràng thấy sự khác biệt trong điều này, mặc dù cùng địa chỉ 172.28.24.199 và cùng port 80 nhưng ở những vị trí truy cập khác nhau thì cho kết quả khác nhau.

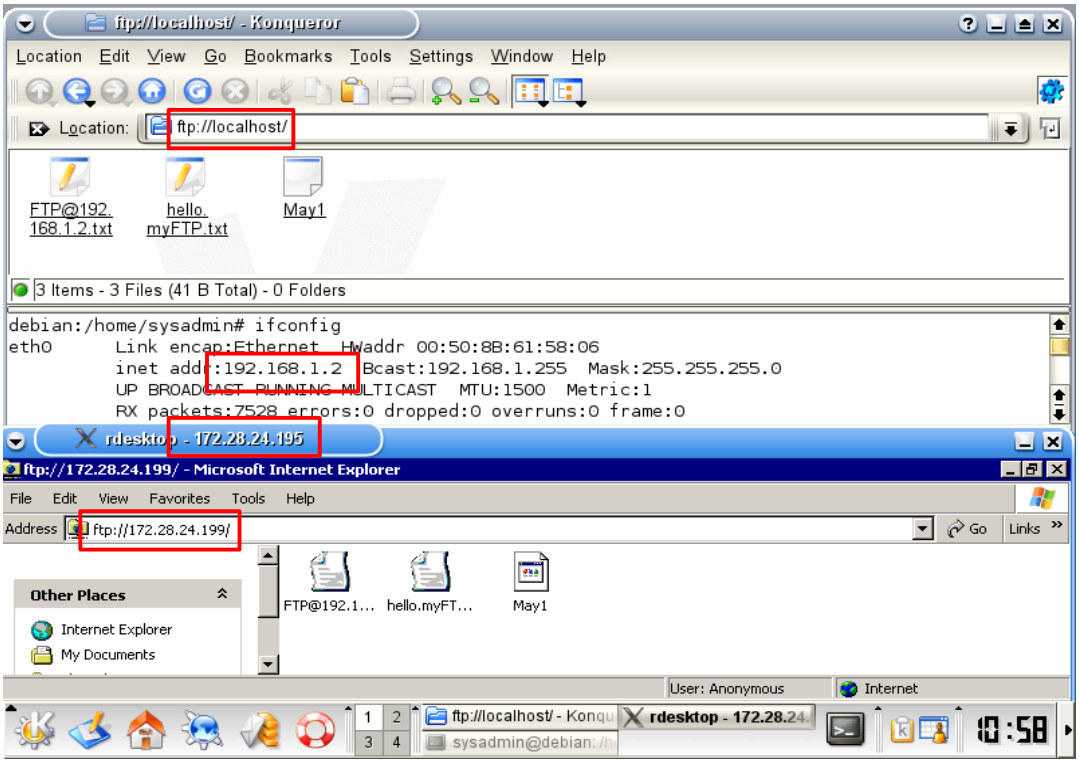
Tương tự như trên, trên máy 192.168.1.2 ta truy cập ftp://localhost và đăng nhập từ xa đến máy ở mạng khác và dùng Internet Explorer để truy cập ftp://172.28.24.199. Cả 2 điều này cùng có nghĩa là truy cập đến FTP Server trên máy 192.168.1.2 port 21. Do đó, ta nhận được hai kết quả giống nhau.



Hình 3: Kết quả truy cập Web Server trên 2 máy khác nhau



Hình 4:Kết quả truy cập Web Server trên máy dùng làm gateway



Hình 5: Kết quả truy cập ftp đồng thời trên 2 máy

Kết quả trên máy dùng làm gateway, chúng tôi dùng chương trình tcpdump giám giám việc định tuyến qua gateway. Kết quả thu được như sau:

11:01:09.614831 172.28.24.199.1065 > 172.28.24.195.3389: . ack 309 win 53576 <nop,nop,timestamp 589252 23626> (DF)
11:01:09.908869 172.28.24.199.1026 > www.hcmut.edu.vn.domain: 59879+ PTR? 164.24.28.172.in-addr.arpa. (44) (DF)
11:01:09.909556 www.hcmut.edu.vn.domain > 172.28.24.199.1026: 59879 NXDomain* 0/1/0 (112) (DF)
11:01:09.925041 172.28.24.195.3389 > 172.28.24.199.1065: P 309:326(17) ack 1 win 64376 <nop,nop,timestamp 23629 589252> (DF)
11:01:09.925202 172.28.24.199.1065 > 172.28.24.195.3389: . ack 326 win 53576 <nop,nop,timestamp 589283 23629> (DF)
11:01:10.455809 172.28.24.195.3389 > 172.28.24.199.1065: P 326:342(16) ack 1 win 64376 <nop,nop,timestamp 23634 589283> (DF)
11:01:10.455995 172.28.24.199.1065 > 172.28.24.195.3389: . ack 342 win 53576 <nop,nop,timestamp 589336 23634> (DF)
11:01:10.555978 172.28.24.195.3389 > 172.28.24.199.1065: P 342:371(29) ack 1 win 64376 <nop,nop,timestamp 23635 589336> (DF)
11:01:10.556143 172.28.24.199.1065 > 172.28.24.195.3389: . ack 371 win 53576 <nop,nop,timestamp 589346 23635> (DF)
11:01:10.986546 172.28.24.195.3389 > 172.28.24.199.1065: P 371:388(17) ack 1 win 64376 <nop,nop,timestamp 23640 589346> (DF)
11:01:10.986722 172.28.24.199.1065 > 172.28.24.195.3389: . ack 388 win 53576 <nop,nop,timestamp 589389 23640> (DF)
11:01:11.517327 172.28.24.195.3389 > 172.28.24.199.1065: P 388:404(16) ack 1 win 64376 <nop,nop,timestamp 23646 589389> (DF)
11:01:11.517490 172.28.24.199.1065 > 172.28.24.195.3389: . ack 404 win 53576 <nop,nop,timestamp 589442 23646> (DF),nop,timestamp 23626 589230> (DF)
11:01:09.614831 172.28.24.199.1065 > 172.28.24.195.3389: . ack 309 win 53576 <nop,nop,timestamp 589252 23626> (DF)
11:01:09.908869 172.28.24.199.1026 > www.hcmut.edu.vn.domain: 59879+ PTR? 164.24.28.172.in-addr.arpa. (44) (DF)
11:01:09.909556 www.hcmut.edu.vn.domain > 172.28.24.199.1026: 59879 NXDomain* 0/1/0 (112) (DF)
11:01:09.925041 172.28.24.195.3389 > 172.28.24.199.1065: P 309:326(17) ack 1 win 64376 <nop,nop,timestamp 23629 589252> (DF)
11:01:09.925202 172.28.24.199.1065 > 172.28.24.195.3389: . ack 326 win 53576 <nop,nop,timestamp 589283 23629> (DF)
11:01:10.455809 172.28.24.195.3389 > 172.28.24.199.1065: P 326:342(16) ack 1 win 64376 <nop,nop,timestamp 23634 589283> (DF)
11:01:10.455995 172.28.24.199.1065 > 172.28.24.195.3389: . ack 342 win 53576 <nop,nop,timestamp 589336 23634> (DF)
11:01:10.555978 172.28.24.195.3389 > 172.28.24.199.1065: P 342:371(29) ack 1 win 64376 <nop,nop,timestamp 23635 589336> (DF)
11:01:10.556143 172.28.24.199.1065 > 172.28.24.195.3389: . ack 371 win 53576 <nop,nop,timestamp 589346 23635> (DF)

```
11:01:10.986546 172.28.24.195.3389 > 172.28.24.199.1065: P 371:388(17) ack 1 win 64376
<nop,nop,timestamp 23640 589346> (DF)
11:01:10.986722 172.28.24.199.1065 > 172.28.24.195.3389: . ack 388 win 53576
<nop,nop,timestamp 589389 23640> (DF)
11:01:11.517327 172.28.24.195.3389 > 172.28.24.199.1065: P 388:404(16) ack 1 win 64376
<nop,nop,timestamp 23646 589389> (DF)
11:01:11.517490 172.28.24.199.1065 > 172.28.24.195.3389: . ack 404 win 53576
<nop,nop,timestamp 589442 23646> (DF)
```

Kết quả trên cho thấy ta hoàn toàn không thấy được những máy trên mạng 192.168.1.0/24.

Tóm lại, dùng iptables để cấu hình việc NAT từ trong ra ngoài để cho phép từ những máy trong mạng LAN có thể truy cập đến các Server bên ngoài. Và việc NAT từ ngoài vào trong là để cho phép các máy có thể ở ngoài mạng có thể truy cập đến những Server bên trong mạng LAN. Kết quả cho thấy, ta đã thực hiện được cân bằng tải server, tức là cùng địa chỉ IP nhưng khác port, ta có thể truy cập đến 2 server khác nhau. Thứ hai, là nếu với những cách truy cập khác nhau và ở những vị trí khác nhau thì máy tính cũng sẽ hiểu khác nhau. Và thức ba là, từ kết quả của chương trình tcpdump cho thấy với iptables ta ngoài việc thực hiện lọc gói tin, nó còn thực hiện được NAT và đồng thời vẫn đảm bảo tính bảo mật cho mạng bên trong. Tuy nhiên, việc cấu hình cân bằng tải server và bảo mật cho mạng người ta không làm trên phần mềm mà làm trực tiếp trên các phần cứng.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Thị Điệp và Tiêu Đông Nhơn, *Giáo trình Dịch vụ mạng Linux,* Đại học Quốc Gia Thành phố Hồ Chí Minh 12/2005

[2] How do i forward ftp from my firewall to an internal server by Mark E. Donaldson

[3] PORT FORWARDING - with IPTABLES while using BASTILLE firewall by kishan at hackorama dot com

[4] Masquerading Made Simple HOWTO by John Tapsell, Thomas Spellman and Matthias Grimm