

TRUNG TÂM ĐÀO TẠO NEWSTAR

Newstar

**QUẢN TRỊ
HỆ THỐNG**

LINUX

LPI 2



Biên soạn: HUỲNH THANH TÂM

TRUNG TÂM ĐÀO TẠO NEWSTAR



Quản trị hệ thống LINUX

(LPI 2)

Biên soạn: Huỳnh Thanh Tâm

8-2017

Mục Lục

B. LBI 2

Chương 14: WEBMIN	2
Chương 15: VNC SERVER.....	4
Chương 16: DHCP SERVER	7
Chương 17: SAMBA.....	10
Chương 18: NFS SERVER	13
Chương 19: DNS	15
Chương 20: MAIL SERVER	23
Chương 21: SQUID PROXY	28
Chương 22: APACHE WEB SERVER	33
Chương 23: IPTABLES.....	35

newstar.vn

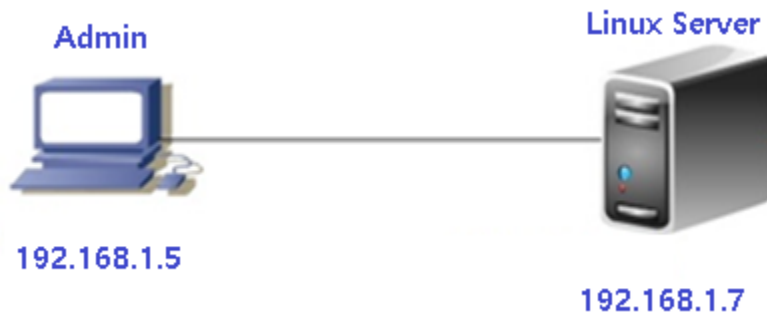
Chương 14: WEBMIN

1) Giới thiệu WebMin

Webmin là phần mềm quản trị server linux qua giao diện đồ họa. Cho phép người quản trị dễ dàng quản lý tài nguyên và cấu hình các dịch vụ thông qua giao diện web như: User management, Disk management, Network, Iptables (Firewall), Cron, Apache, DNS....

Mặc định Web min sử dụng cổng 10000 để giao tiếp.

2) Mô hình triển khai:



3) Cài đặt

❖ Cài trực tiếp từ internet

Chú ý: Linux Server phải đi được internet. Tắt Firewall (sẽ học ở chương sau)

Bước 1: Tạo file webmin.repo tại thư mục /etc/yum.repos.d/

#vi /etc/yum.repos.d/webmin.repo

```
[Webmin]
name=Webmin Distribution Neutral
#baseurl=http://download.webmin.com/download/yum
mirrorlist=http://download.webmin.com/download/yum/mirrorlist
enabled=1
```

Bước 2: Import PGP Key của webmin

#rpm --import <http://www.webmin.com/jcameron-key.asc>

Bước 3: Cài đặt Webmin

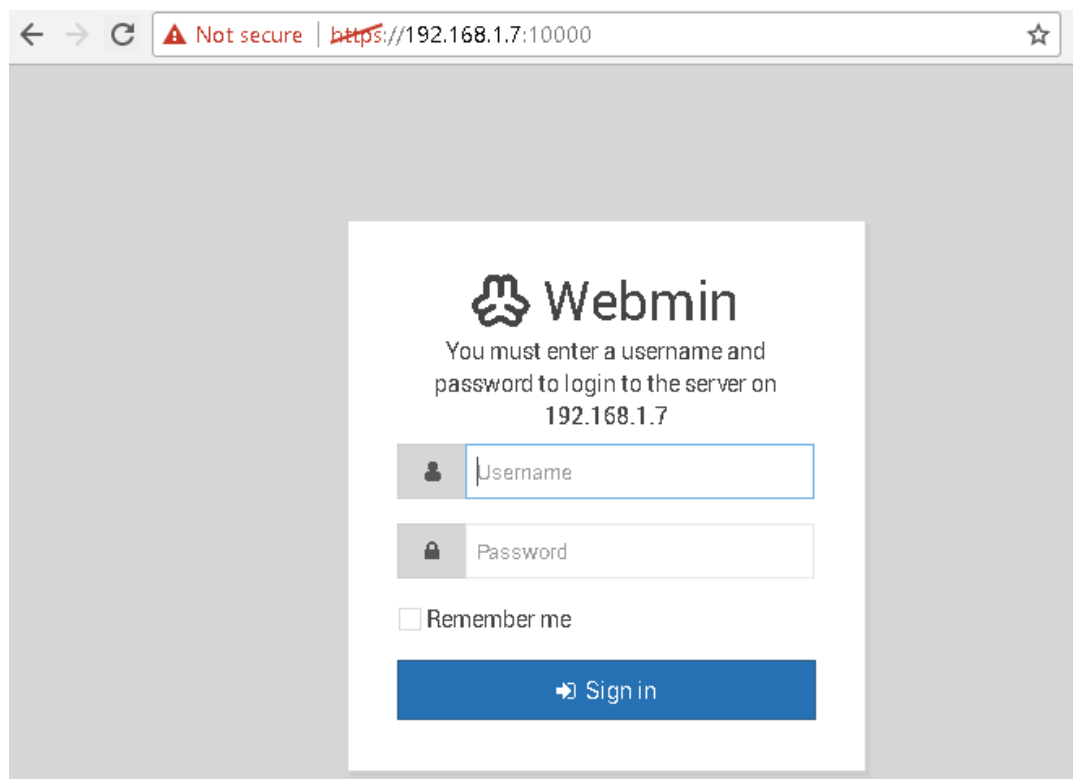
```
#yum -y install webmin
```

Bước 4: khởi động dịch vụ Webmin và cho khởi động cùng HĐH

```
#service webmin start
```

```
#chkconfig webmin on
```

Bước 5: kiểm tra truy cập từ Admin



❖ **Cài đặt từ rpm:**

Bước 1: Download webmin

```
#wget http://prdownloads.sourceforge.net/webadmin/webmin-1.840-1.noarch.rpm
```

Bước 2: Cài đặt các gói thư viện cần thiết

```
#yum -y install perl perl-Net-SSLeay openssl perl-IO-Tty perl-Encode-Detect
```

Bước 3: Cài đặt webmin

```
#rpm -ivh webmin-1.840-1.noarch.rpm
```

Bài tập:

- Chỉ cho phép lớp 192.168.1.0/24 truy cập đến webmin. Cấm tất cả các IP khác
- Phân quyền truy cập các chức năng của Wemin cho từng user quản trị

Chương 15: VNC SERVER

1) Giới thiệu VNC

VNC – Virtual Network Computing là một công cụ phổ biến để cung cấp truy cập Server từ xa thông qua giao diện đồ họa..

2) Mô hình



3) Cài đặt và cấu hình

Bước 1: Cài đặt tigervnc-server từ internet

```
#yum install tigervnc-server
```

Bước 2: Cấu hình cho phép 2 user root và nam truy cập vào VNC-Server

✓ Tạo file cấu hình vnc cho user **root** bằng cách copy file cấu hình mẫu của dịch vụ

```
#cp /lib/systemd/system/vncserver@.service
```

```
/etc/systemd/system/vncserver@:1.service
```

✓ Mở file và chỉnh sửa tên user thành **root** và đổi đường thư mục home của user root

```
#vi /etc/systemd/system/vncserver@:1.service
```

(chỉnh sửa theo nội dung bên dưới)

```
ExecStart=/sbin/runuser -l root -c "/usr/bin/vncserver %i"
```

```
PIDFile=/root/.vnc/%H%i.pid
```

✓ Tạo file cấu hình vnc cho user **nam**

```
#cp /lib/systemd/system/vncserver@.service
```

```
/etc/systemd/system/vncserver@:2.service
```

✓ Mở file và chỉnh sửa tên user thành **nam** và đổi đường thư mục home của user

nam

```
#vi /etc/systemd/system/vncserver@:1.service
```

(chỉnh sửa theo nội dung bên dưới)

```
ExecStart=/sbin/runuser -l nam -c "/usr/bin/vncserver %i"
```

```
PIDFile=/home/nam/.vnc/%H%i.pid
```

✓ Tạo user nam

```
#useradd nam
```

✓ Đặt password VNC cho user root

```
#vncpasswd
```

✓ Đặt password VNC cho user nam

```
#su nam
```

```
#vncpasswd
```

✓ Reload lại dịch vụ

```
#systemctl daemon-reload
```

✓ Khởi động dịch vụ vnc cho user nam và root

```
#systemctl start vncserver@:1.service
```

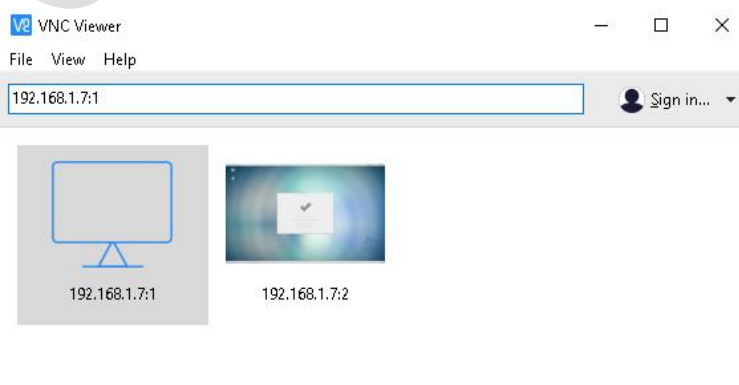
```
#systemctl start vncserver@:2.service
```

✓ Khởi động khi hệ thống startup

```
#systemctl enable vncserver@:1.service
```

```
#systemctl enable vncserver@:2.service
```

Bước 3: Kiểm tra hoạt động của VNC. Máy admin download VNC-Viewer và truy cập bằng user: root (192.168.1.7:1)



VNC 192.168.1.7:1 - VNC Viewer

VNC Authentication

VNC Server: 192.168.1.7::5901

Username:

Password:

Remember password

OK Cancel

Stop

VNC bằng user: nam

VNC Viewer

File View Help

192.168.1.7:2 Sign in...



192.168.1.7:1



192.168.1.7:2

VNC 192.168.1.7:2 - VNC Viewer

VNC Authentication

VNC Server: 192.168.1.7::5902

Username:

Password:

Remember password

OK Cancel

Stop

Chương 16: DHCP SERVER

1) Giới thiệu:

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL) là dịch vụ cấp phát địa chỉ IP tự động cho các máy tính hoạt động theo mô hình server-client, máy cấu hình DHCP Server phải được gán IP tĩnh. Thông tin mà client nhận được từ DHCP server gồm: IP, subnet mask, default gateway, DNS server, ...

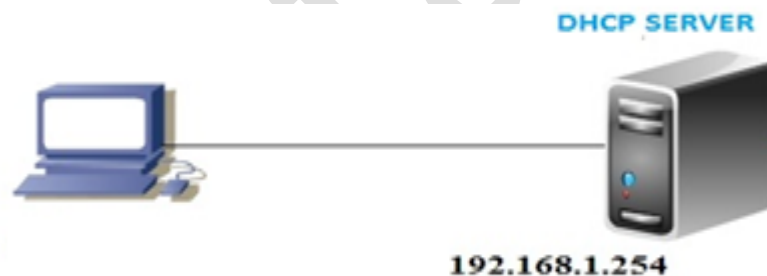
Các địa chỉ IP trong mạng LAN được đặt theo RFC 1918:

Class A: 10.0.0.0 – 10.255.255.255 (10/8 prefix)

Class B: 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)

Class C: 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

2) Mô hình triển khai



(Chú ý: tắt dhcp trên VMWare)

3) Cài đặt

- Thiết lập địa chỉ IP tĩnh cho DHCP Server: 192.168.1.254/24
- Cài từ internet:

```
#yum install dhcp
```

- Cài từ CDROM:

```
#rpm -ivh dhcp-4.1.1-25P1.el6.i686.rpm
```

4) Cấu hình

A. DHCP-Server

Bước 1: copy file cấu hình

```
#cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf  
cp: overwrite '/etc/dhcp/dhcpd.conf'? Chọn y
```

Bước 2: Tùy chỉnh các thông số

```
#vi /etc/dhcp/dhcpd.conf
```

Bước 3: Xóa nội dung từ dòng 23 đến cuối file

Bước 4: Thêm nội dung sau vào cuối file

```
subnet 192.168.1.0 netmask 255.255.255.0{  
    option routers 192.168.1.1;  
    option subnet-mask 255.255.255.0;  
    option domain-name-servers 8.8.8.8;  
    range 192.168.1.100 192.168.1.200;  
    default-lease-time 21600;  
    max-lease-time 43200;  
}
```

Khởi động lại dịch vụ

```
#systemctl start dhcpd
```

Cho dịch vụ khởi động cùng với HĐH

```
# systemctl enable dhcpd
```

B. DHCP Client

Windows OS

- `ipconfig /release`
- `ipconfig /renew`
- `ipconfig`

Linux OS

- `dhclient eth0`
- `dhclient -r`
- `ifconfig`

Thực hiện cấp ip theo Mac-Address:

```
subnet 192.168.1.0 netmask 255.255.255.0{
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option domain-name-servers 8.8.8.8;
range 192.168.1.100 192.168.1.200;
default-lease-time 21600;
max-lease-time 43200;
host nsshare
{
    hardware ethernet 00:50:56:c0:00:01;
    fixed-address 192.168.1.151;
}
}
```

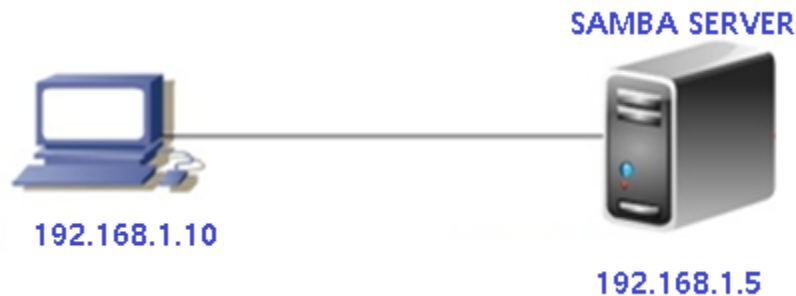
Chương 17: SAMBA

1) Giới thiệu

Samba là dịch vụ của hệ điều hành Linux, chạy trên nền giao thức SMB (Server Message Block) cho phép chia sẻ file hệ thống, máy in với các máy chạy hệ điều hành Windows

Samba Server port numbers: *137/tcp; 137/udp; 138/tcp; 138/udp; 139/udp; 139/udp; 445/tcp; 445/udp*

2) Mô hình



3) Cài đặt SAMBA Server

✓ Cài từ internet:

```
#yum install samba
```

✓ Cài từ đĩa CD:

```
#rpm -ivh samba-3.5.10-114.el6.i686.rpm
```

4) Cấu hình SAMBA Server

Trường hợp 1: Không cần username/password để truy cập dữ liệu chia sẻ

- Tạo một thư mục để thực hiện share dữ liệu.

Ví dụ: Tạo thư mục có tên là “soft”. Trong thư mục soft, tạo thư mục có tên linux1

```
#mkdir /soft
```

```
#mkdir /soft/linux2
```

Phân quyền thư mục soft:

```
#chmod 777 -R /soft/
```

- Cấu hình Server:

#vi /etc/samba/smb.conf

Thêm vào dòng sau vào vị trí dòng số 125

map to guest = bad user

Di chuyển cuối file và thêm nội dung sau

```
[Soft Newstar]
comment = Ung dung van phong
path = /soft
writable = yes
read only = yes
create mode = 0600
directory mode = 0700
guest ok = yes
```

Các options:

guest ok: cho phép clients kết nối tới thư mục file được chia sẻ mà không cần password.

create mode: Quyền hạn của file khi được tạo file

directory mode: Quyền hạn của thư mục khi được tạo

Kiểm tra cấu hình vừa thiết lập

#testparm

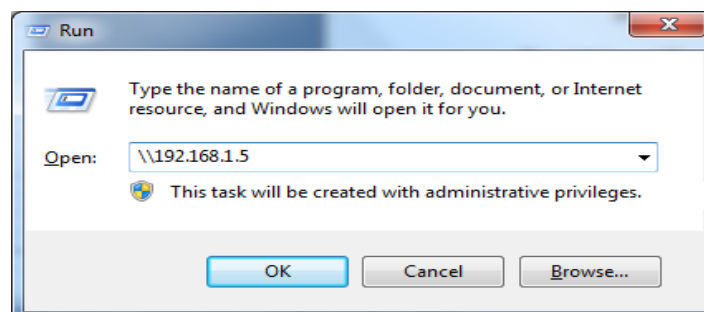
Khởi động dịch vụ samba

#systemctl restart smb.service

Kiểm tra trạng thái samba

#smbstatus

A. Client Test (Windows):



Trường hợp 2: cần chứng thực để truy cập dữ liệu chia sẻ

- Tạo thư mục chia sẻ

```
#mkdir /ketoan
```

- Tạo group kế toán, và thêm user kt1 vào nhóm này

```
#groupadd ketoan
```

```
#useradd -g ketoan kt1
```

- Tạo password samba cho user kt1

```
#smbpasswd -a kt1
```

- Chỉnh sửa file cấu hình

```
#vi /etc/samba/smb.conf
```

```
[Phong Ke Toan]
```

```
comment = tai lieu p.ketoan
```

```
path = /ketoan
```

```
valid users = @ketoan
```

```
writable = yes
```

```
guest ok = no
```

(chú ý: xóa cache user/pass truy cập trên windows : `net use */delete`)

Chương 18: NFS SERVER

1) Giới thiệu

NFS(Network File System) là dịch vụ chia sẻ file trên các hệ thống Unix/Linux. Dịch vụ NFS cho phép chia sẻ tập tin cho nhiều người dùng trên cùng mạng và người dùng có thể thao tác như với tập tin trên chính đĩa cứng của mình

2) Mô hình



3) Cài đặt và cấu hình

A. Server

Bước 1: Cài các gói sau từ internet

```
#yum install nfs-utils nfs-utils-lib portmap
```

Bước 2: Tạo thư mục chia sẻ

```
#mkdir /soft
```

```
#mkdir /giaitri
```

```
#mkdir /data
```

Bước 3: Cấu hình thư mục chia sẻ /soft

```
#vi /etc/exports
```

Cấu trúc file exports như sau:

```
/Thư mục chia sẻ host1(options) host2(option)
```

Các tùy chọn thông dụng:

- ✓ *ro*: thuộc tính chỉ đọc
- ✓ *rw*: thuộc tính đọc và ghi
- ✓ *sync*: đồng bộ dữ liệu

- ✓ *root_squash*: không cho phép sử dụng hệ thống với quyền hạn root
- ✓ *no_root_squash*: ngược lại với *root_squash*
- ✓ ...

(Dùng #man exports để xem các options khác)

Nội dung file /etc/exports với mục đích chỉ cho phép các ip thuộc lớp mạng 192.168.1.0/24 có quyền đọc.

```
/soft 192.168.1.0/24(rw,sync)
```

```
/data 192.168.1.5(rw,sync)
```

```
/giaitri 192.168.1.5(ro,root_squash,sync)
```

Bước 4: Khởi động dịch vụ

```
#service nfs start
```

Reload lại toàn bộ cấu hình cho nfs

```
#exportfs -a
```

(Nếu chỉ muốn cập nhật các entry vừa thêm ta dùng lệnh

```
#exportfs -r)
```

B. Client (Linux)

Bước 1: kiểm tra thông tin dịch vụ NFS và danh sách các thư mục được export trên NFS Server

```
#showmount -e 192.168.1.5
```

Bước 2: Tạo thư mục để làm mount point

```
#mkdir /mnt/a1
```

```
#mkdir /mnt/a2
```

```
#mkdir /mnt/a3
```

Bước 2: thực hiện mount thư mục share về máy

```
#mount -t nfs 192.168.1.5:/soft /mnt/a1
```

```
#mount -t nfs 192.168.1.5:/data /mnt/a2
```

```
#mount -t nfs 192.168.1.5:/giaitri /mnt/a3
```

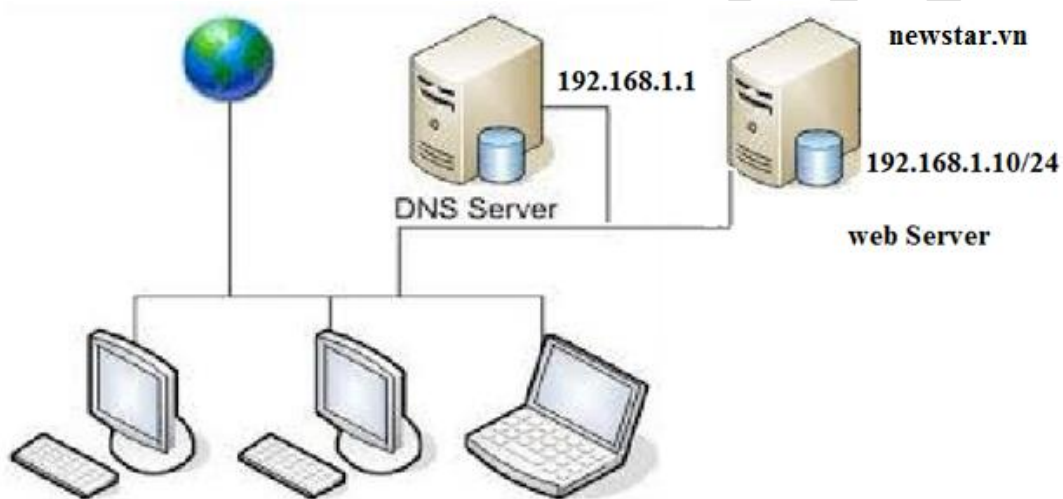

Chương 19: DNS

1) Giới thiệu

DNS (Domain Name System) là hệ thống phân giải tên miền được phát minh vào năm 1984 cho Internet, cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền.

2) Mô hình

sử dụng 1 Server DNS dùng để phân giải tên miền của 1 WebServer



Chuẩn bị hệ thống:

Server	OS
DNS Server (192.168.1.1)	Centos 7.X
WebServer (192.168.1.10)	Centos 7.X
client	Win 7 or Win 8 (test)

Cài đặt và cấu hình DNS (192.168.1.1):

Bước 1: Đặt hostname cho Server DNS là: dns1.newstar.vn và restart lại Server

```
#vi /etc/sysconfig/network
```

```
HOSTNAME=dns1.newstar.vn
```

```
#init 6
```

Bước 2: Cài đặt các gói bind*

```
#yum install bind*
```

Bước 3: Cấu hình file named.conf

```
#vi /etc/named.conf
```

```
options {
    listen-on port 53 { 192.168.1.1 };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file      "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query    { any; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;
}
```

Bước 4: Cấu hình các Zone cho DNS Server

```
#vi /etc/named.rfc1912.zones
```

(Xuống cuối file cấu hình zone phân giải thuận và phân giải nghịch)

```
zone "newstar.vn" IN {
    type master;
    file "newstar.vn.zone";
    allow-update { none; };
    allow-query { any; };
};
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "newstar.vn.rr.zone";
    allow-update { none; };
    allow-query { any; };
};
```

Bước 5: Tạo các file CSDL cho zone thuận và zone nghịch vừa khai báo

(copy file mẫu từ chương trình cài đặt và sửa lại nội dung cho phù hợp)

```
#cp /var/named/named.localhost /var/named/newstar.vn.zone
```

```
#cp /var/named/named.loopback /var/named/newstar.vn.rr.zone
```

```
#vi /var/named/newstar.vn.zone
```

```
$TTL 1D
@      IN SOA  dns1.newstar.vn. root.newstar.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

      IN NS  dns1.newstar.vn.
newstar.vn.  IN A  192.168.1.10
dns1        IN A  192.168.1.1
web         IN A  192.168.1.10
```

#vi /var/named/newstar.vn.rr.zone

```
$TTL 1D
@      IN SOA  dns1.newstar.vn. root.newstar.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

      IN NS  dns1.newstar.vn.
1      IN PTR dns1.newstar.vn.
10     IN PTR web.newstar.vn.
```

Bước 6: Gán quyền trên 2 file zone vừa tạo

#cd /var/named/

#chown named:named newstar.vn.zone

#chown named:named newstar.vn.rr.zone

Bước 7: Restart dịch vụ named

#service named restart

#systemctl enable named

Cài đặt Web Server (192.168.1.10)

Bước 1: Cài đặt gói httpd

#yum install httpd

Bước 2: Chỉnh sửa file httpd.conf

#vi /etc/httpd/conf/httpd.conf

(Thêm vào cuối file nội dung sau)

*<VirtualHost *:80>*

DocumentRoot /var/www/newstar

ServerName newstar.vn

ServerAlias www.newstar.vn

</VirtualHost>

Bước 3: Tạo file index.htm có nội dung tùy ý trong /var/www/newstar

Bước 4: Restart dịch vụ

service httpd restart

Bước 5: Trỏ DNS về ip Server DNS

#vi /etc/resolv.conf

nameserver 192.168.1.1

TEST DNS trên máy Client

Vào terminal

#nslookup newstar.vn

#nslookup dns1.newstar.vn

Truy cập web newstar.vn

B-Mô hình sử dụng 2 Server DNS (primary secondary)

- ✓ DNS Primary (192.168.1.1)
- ✓ DNS Secondary (192.168.1.2)
- ✓ Web Server (192.168.1.10)

Cài đặt gói bind cho 2 máy Primary và secondary:

Cài từ Internet:

```
#yum install bind*
```

Cấu hình cho DNS cho primary:

Bước 1: Xem nội dung file named.conf

```
#vi /etc/named.conf
```

Bước 2: thêm nội dung vào file named.rfc1912.zones

```
#vi /etc/named.rfc1912.zones
```

Thêm vào cuối file

```
zone "newstar.vn" IN {  
    type master;  
    file "newstar.vn.zone";  
    allow-transfer {192.168.1.2;};  
    allow-update {192.168.1.2;};  
    allow-query {any;};  
};  
  
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "newstar.vn.rr.zone";  
    allow-transfer {192.168.1.2;};  
    allow-update {192.168.1.2;};  
    allow-query {any;};  
};
```

Bước 3: Copy và đổi tên 2 file sau:

```
#cp /var/named/named.localhost /var/named/newstar.vn.zone
```

```
#cp /var/named/named.loopback /var/named/newstar.vn.rr.zone
```

Bước 4: Chỉnh sửa file cấu hình cho file phân giải thuận *newstar.vn.zone*

```
#vi /var/named/newstar.vn.zone
```

(NS dùng để khai báo máy chủ DNS của 1 tên miền)

(A: ánh xạ tên host vào 1 ip)

```
$TTL 1D
```

```
@ IN SOA dns1.newstar.vn. root.newstar.vn. (
```

```
0 ; serial
```

```
1D ; refresh
```

```
1H ; retry
```

```
1W ; expire
```

```
3H ) ; minimum
```

```
IN NS dns1.newstar.com.
```

```
IN NS dns2.newstar.com.
```

```
newstar.vn. IN A 192.168.1.10
```

```
www IN CNAME newstar.vn
```

```
dns1 IN A 192.168.1.1
```

```
dns2 IN A 192.168.1.2
```

Bước 5: Cấu hình file phân giải nghịch

```
# vi /var/named/newstar.vn.rr.zone
```

```
$TTL 1D
```

```
@ IN SOA dns1.newstar.vn. root.newstar.vn. (
```

```
0 ; serial
```

```
1D ; refresh
```

```
1H ; retry
```

```
1W ; expire
```

3H) ; minimum

IN NS dns1.newstar.vn.

IN NS dns2.newstar.vn.

1 IN PTR dns1.newstar.vn.

2 IN PTR dns2.newstar.vn.

10 IN PTR newstar.vn.

Bước 6: Khởi động dịch vụ named khi boot Server

chkconfig named on

Bước 7: gán nhóm sở hữu cho user named vào các file vừa tạo

#chgrp named newstar*

Bước 8: Khởi động daemon **named** cho quá trình làm việc

#/etc/init.d/named start

Bước 9: Cấu hình file phân giải domain

#vi /etc/resolv.conf

(thêm vào dòng sau)

nameserver 192.168.1.1

Bước 10: Kiểm tra phân giải DNS

#nslookup newstar.vn

Cấu hình Secondary DNS Server

Khai báo zone thuận và zone nghịch từ dns1.newstar.vn

Bước 1: cấu hình file dns

#vi /etc/named.rfc1912.zones

(Thêm vào cuối file dòng sau)

zone "newstar.vn" IN {

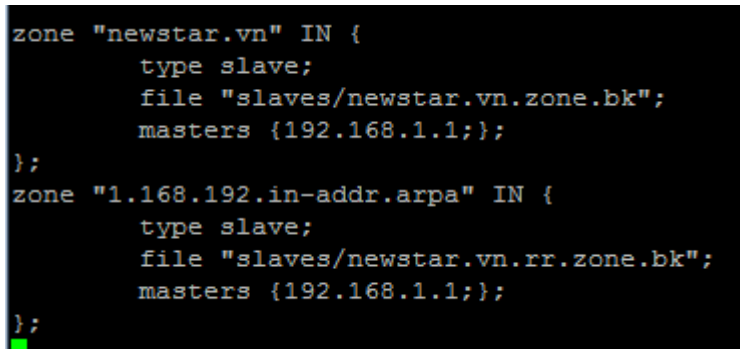
type slave;

file "slaves/newstar.vn.zone.bk";

masters {192.168.1.1};

};

```
zone "1.168.192.in-addr.arpa" IN {  
    type slave;  
    file "slaves/newstar.vn.rr.zone.bk";  
    masters {192.168.1.1;};  
};
```



```
zone "newstar.vn" IN {  
    type slave;  
    file "slaves/newstar.vn.zone.bk";  
    masters {192.168.1.1;};  
};  
zone "1.168.192.in-addr.arpa" IN {  
    type slave;  
    file "slaves/newstar.vn.rr.zone.bk";  
    masters {192.168.1.1;};  
};
```

Bước 2: Kiểm tra lại

```
#ls -l /var/named/slaves/
```

Bước 3: Restart dịch vụ

```
#/etc/init.d/named restart
```

Bước 4: Kiểm tra lại nội dung thư mục slaves

```
#ls -l /var/named/slaves/
```

Bước 5: Xem nội dung zone thuận transfer từ master dns

```
#vi /var/named/slaves/newstar.vn.zone.bk
```

Bước 6: Cấu hình nameserver

```
# vi /etc/resolv.conf
```

(Thêm vào)

```
nameserver 192.168.1.1
```

```
nameserver 192.168.1.2
```

Bước 7: Thực hiện kiểm tra dns

```
# nslookup newstar.vn
```

Bước 8: tắt máy dns1 và thực hiện kiểm tra lại dns (nslookup)

Chương 20: MAIL SERVER

(Postfix, Dovecot and SquirrelMail)

1) Giới thiệu

Mail server cho phép user gửi nhận thư điện tử. Mail server sẽ quản lý toàn bộ các tài khoản email trong hệ thống nội bộ.

2) Cài đặt

Bước 1: Đặt hostname cho Server Mail là: mail.newstar.vn

```
#nmtui
```

```
Update repository
```

```
#yum install epel-release
```

Bước 2: Cài đặt gói postfix

```
#yum install postfix
```

Bước 3: cấu hình file postfix

```
# vi /etc/postfix/main.cf
```

```
(dòng 76)
```

```
myhostname = mail.newstar.vn
```

```
(dòng83 )
```

```
mydomain = newstar.vn
```

```
(dòng 99)
```

```
myorigin = $mydomain
```

```
(dòng 113)
```

```
inet_interfaces = all
```

```
(dòng 119)
```

```
inet_protocols = all
```

```
(dòng 164 – comment)
```

```
#mydestination = $myhostname, localhost.$mydomain, localhost
```

```
(dòng 165 - uncomment)
```

```
mydestination = $myhostname, localhost.$mydomain, localhost, newstar.vn  
(dòng 264)
```

```
mynetworks = 168.100.189.0/28, 127.0.0.0/8, 0.0.0.0/0  
(dòng 419 – bỏ dấu #)
```

```
home_mailbox = Maildir/
```

Bước 4: start dịch vụ postfix

```
#systemctl enable postfix
```

```
#systemctl restart postfix
```

Bước 5: Test postfix

```
[root@mail ~]# netstat -an | grep :25  
tcp      0      0 0.0.0.0:25          0.0.0.0:*          LISTEN  
tcp      0      0 :::25              :::*                LISTEN
```

Bước 6: Cài đặt gói dovecot

```
# yum install dovecot
```

Bước 7: cấu hình dovecot

```
#vi /etc/dovecot/dovecot.conf
```

(dòng 24)

```
protocols = imap pop3 lmtp
```

```
# vi /etc/dovecot/conf.d/10-mail.conf
```

(dòng 24 – bỏ dấu #)

```
mail_location = maildir:~/Maildir
```

```
#vi /etc/dovecot/conf.d/10-auth.conf
```

(dòng 10)

```
disable_plaintext_auth = yes
```

(dòng 100)

```
auth_mechanisms = plain login
```

```
# vi /etc/dovecot/conf.d/10-master.conf
```

(dòng 91,92)

```
user = postfix
```

```
group = postfix
```

Bước 8: Start dịch vụ dovecot

```
# systemctl restart dovecot
```

```
# systemctl enable dovecot
```

Bước 9: install squirrelmail

```
# yum install squirrelmail
```

```
# service httpd start
```

```
#chkconfig httpd on
```

Bước 10: cấu hình Squirrelmail

```
# cd /usr/share/squirrelmail/config/
```

```
./conf.pl
```

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C  Turn color off
S  Save data
Q  Quit

Command >> █
```

Chọn 1

Thiết lập các thông số

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Organization Preferences
1. Organization Name      : newstar
2. Organization Logo      : ../images/sm_logo.png
3. Org. Logo Width/Height : (308/111)
4. Organization Title     : Welcome to Newstar webmail
5. Signout Page           :
6. Top Frame              : _top
7. Provider link          : http://newstar.vn
8. Provider name          : newstar

R  Return to Main Menu
C  Turn color off
S  Save data
Q  Quit

Command >> █
```

Sau khi thiết lập xong –chọn R để quay lại menu

Chọn 2 – thiết lập các thông số

```
SquirrelMail Configuration : Read: config.php (1.4.0)
-----
Server Settings

General
-----
1. Domain                : newstar.vn
2. Invert Time            : false
3. Sendmail or SMTP      : SMTP

A. Update IMAP Settings  : localhost:143 (uw)
B. Update SMTP Settings  : localhost:25

R  Return to Main Menu
C  Turn color off
S  Save data
Q  Quit

Command >> █
```

Chọn S để lưu

Chọn Q để thoát

Bước 11: cấu hình http cho mail server

#vi /etc/httpd/conf/httpd.conf

(Thêm vào cuối file nội dung sau)

Alias /squirrelmail /usr/share/squirrelmail

<Directory /usr/share/squirrelmail>

Options Indexes FollowSymLinks

RewriteEngine On

AllowOverride All

DirectoryIndex index.php

Order allow,deny

Allow from all

</Directory>

Bước 12: Restart dịch vụ http

service httpd restart

3) Cấu hình DNS cho Mail Server

a. File forward.zone

```
$TTL 1D
@ IN SOA newstar.vn. root.newstar.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@ IN NS  mail.newstar.vn.
@ IN A   192.168.1.1
mail IN A   192.168.1.1
@ IN MX  10 mail.newstar.vn.
```

b. File reverse.zone

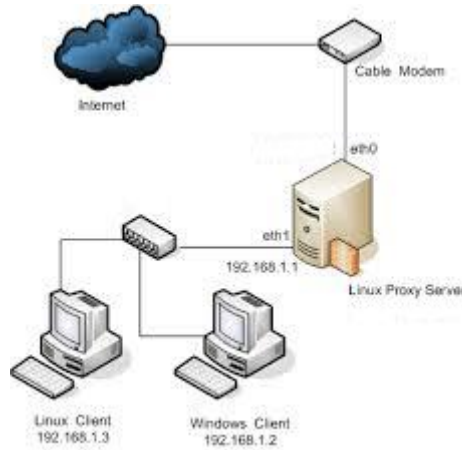
```
$TTL 1D
@ IN SOA newstar.vn. root.newstar.vn. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
@ IN NS  mail.newstar.vn.
1 IN PTR mail.newstar.vn.
```

Chương 21: SQUID PROXY

1) Giới thiệu:

Squid là một proxy server, khả năng của squid là tiết kiệm băng thông (bandwidth), cải tiến việc bảo mật, tăng tốc độ truy cập web cho người sử dụng.

2) Mô hình



3) Chuẩn bị hệ thống

Loại	OS	Ghi chú
Squid Proxy Server	Centos 6.x	2 card mạng. Kết nối được internet eth0: dhcp eth1: 192.168.1.1
Client	XP or Centos	192.168.1.5,20

4) Cài đặt và cấu hình Proxy Server

Bước 1: Cài đặt Squid từ internet

```
#yum install squid
```

Bước 2: File cấu hình

```
#vi /etc/squid/squid.conf
```

(Mặc định Squid Proxy cho phép tất cả các host trong LAN truy cập internet.)

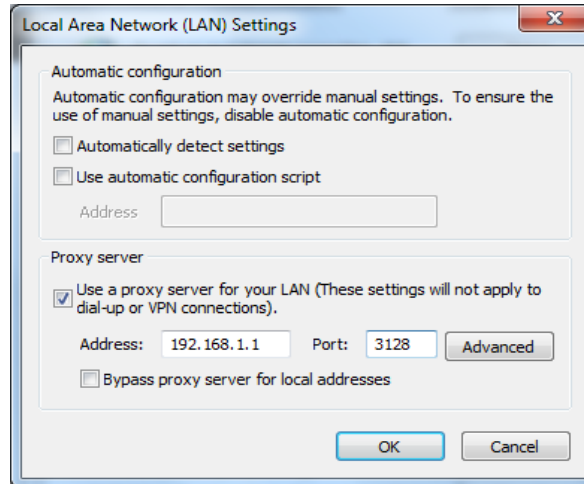
Start squid

```
#services squid start
```

Bước 3: Cấu hình phía client.

Trên client ta cấu hình proxy như sau:

Mở IE, chọn Tools → Internet Options, từ tab Connections chọn LAN Settings...



Thông số trong file *squid.conf*

- *http_port 3128*: Squid lắng nghe trên port 3128

Yêu cầu:

1) Thay đổi port squid lắng nghe là 8080

2) IP của sếp CNTT: 192.168.1.2

- Được phép truy cập vào tất cả các trang web ngoại trừ trang nghe nhạc, xem phim trong thời gian làm việc (sáng từ 8h:12h ; buổi chiều từ 13h:17h30 từ thứ 2 -> thứ 6). Thời gian nghỉ trưa được phép truy cập tất cả.
- Cho phép số kết nối tối đa là 10
- Dung lượng download tối đa 30M
- Dung lượng upload tối đa 30kb

3) IP phòng CNTT 192.168.1.10-100

- Chỉ được truy cập vào các trang web: newstar.vn, dantri.com, 24h.com.vn.
- Thời gian truy cập buổi sáng từ 8h:12h ; buổi chiều từ 13h:17h30.
- Thời gian nghỉ trưa cho phép thêm quyền vào trang **chiasenhac.com** để giải trí

- Trong thời gian làm việc nếu truy cập vào các trang nghe nhạc (chiasenhac.com; nhacso.net) thì tự động redirect đến website newstar.vn

Thực hiện cấu hình:

1) #vi /etc/squid/squid.conf

```
http_port 8080
```

```
#squid -k reconf
```

Thay đổi port trên trình duyệt web proxy setting của client và truy cập lại internet

Từ yêu cầu 2 và 3: thực hiện viết các access-list sau:

```
#các acl định nghĩa các website có keyword trên url
```

```
acl deny-nhac dstdom_regex "/etc/squid/web/denynhac.txt"
```

```
#các acl định nghĩa các dạng file
```

```
acl deny-file-video-nhac url_regex -i /.mp3$/ .mp4$/ .avi$/ .flv$/ .wmv$/ .mp4$
```

```
#định các acl và action cấm xem các video
```

```
acl deny_rep_mime_flashvideo rep_mime_type video/flv
```

```
acl deny_rep_mime_shockwave rep_mime_type ^application/x-shockwave-flash$
```

```
http_reply_access deny deny_rep_mime_flashvideo
```

```
http_reply_access deny deny_rep_mime_shockwave
```

```
#Acl định nghĩa các trang được phép truy cập
```

```
acl allow-web-CNTT dstdomain "/etc/squid/web/webcntt.txt"
```

```
#ACL cho phép vào trang chia se nhạc
```

```
acl allow-mp3-cntt dstdomain "etc/squid/web/giaitricntt.txt"
```

```
#ACL thiết lập thời gian làm việc
```

```
acl time-lam-viec time M T W H F 08:00-11:59
```

```
acl time-lam-viec-chieu time M T W H F 13:00-17:30
```


#ACL thiết lập thời gian nghỉ trưa

acl time-nghe-trua time M T W H F 12:00-12:59

#ACL cho phép số kết nối tối đa là 10

acl sep-max maxconn 10

#ACL định nghĩa IP của Sếp phòng CNTT

acl ip-sep src "/etc/squid/danhsachip/ip-sep.txt"

#ACL định nghĩa IP phòng CNTT

acl ip-cntt src "/etc/squid/danhsachip/ip-cntt.txt"

#Thực hiện yêu cầu quản lý truy cập

#Chính sách cho sếp

http_access deny ip-sep time-lam-viec deny-nhac

http_access deny ip-sep time-lam-viec deny-file-video-nhac

http_access deny ip-sep time-lam-viec-chieu deny-nhac

http_access deny ip-sep time-lam-viec-chieu deny-file-video-nhac

http_access deny ip-sep sep-max

reply_body_max_size 30 MB ip-sep

request_body_max_size 30 kb ip-sep

http_access allow ip-sep

#chính sách cho phòng CNTT

http_access allow ip-cntt time-nghe-trua allow-giaitri-cntt

http_access deny deny-nhac

http_access deny deny-file-video-nhac

http_access deny ip-cntt !allow-web-cntt

http_access allow ip-cntt

#cấu hình redirect

deny_info http://newstar.vn deny-nhac

http_access deny all

#cấu hình cache theo RAM và theo HDD;

#Cache RAM chiếm 32 MB;

#Cache đĩa sử dụng định lưu trữ theo kiểu ufs chiếm 512 MB với 16 thư mục cấp 1

#và 256 thư mục cho mỗi thư mục cấp 1 đó.

cache_dir ufs /var/spool/squid 100 16 256

cache_mem 50 MB

#Thuật toán cache đĩa là heap LFUDA (Least Frequently Used with Dynamic Aging).

#Thuật toán cache ram là heap GDSF (Greedy-Dual Size Frequency)

cache_replacement_policy heap LFUDA

memory_replacement_policy heap GDSF

Nội dung các file .txt đã định nghĩa trong squid.conf

Tên file	Nội dung
denynhac.txt	nhac music mp3
giaitricntt.txt	.chiasenhac.com
webcntt.txt	.newstar.vn .24h.com.vn .dantri.com.vn
ip-cntt.txt	192.168.1.0/24
ip-sep.txt	192.168.1.5

Chương 22: APACHE WEB SERVER

1) Mô hình triển khai



2) Cài đặt

Bước 1: cài đặt các gói httpd

```
#yum install httpd
```

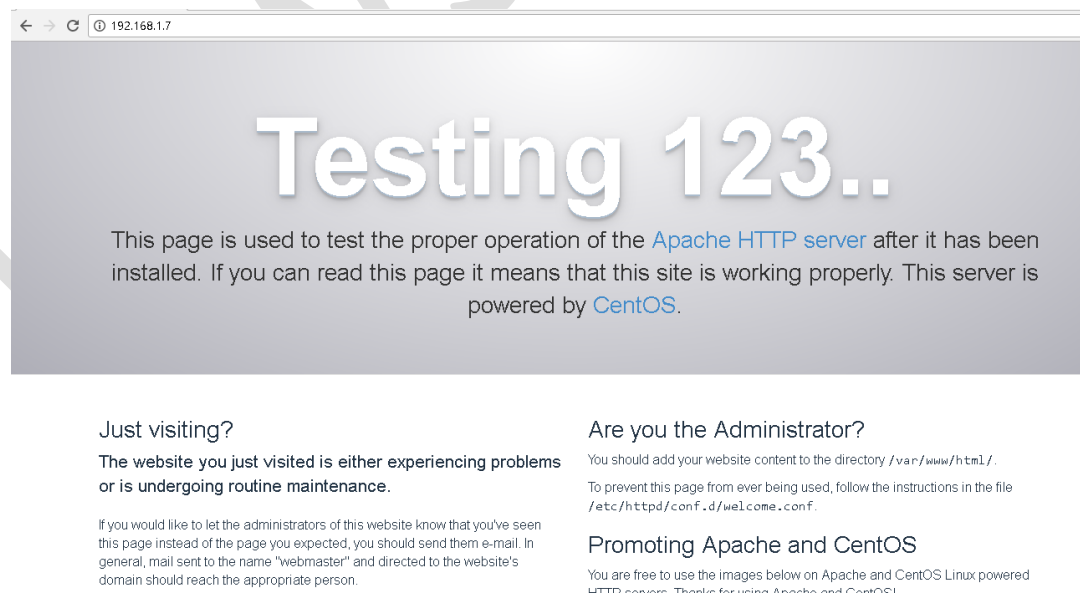
Bước 2: Khởi động dịch vụ

```
#systemctl start httpd
```

```
#chkconfig httpd on
```

Bước 3: Kiểm tra apache

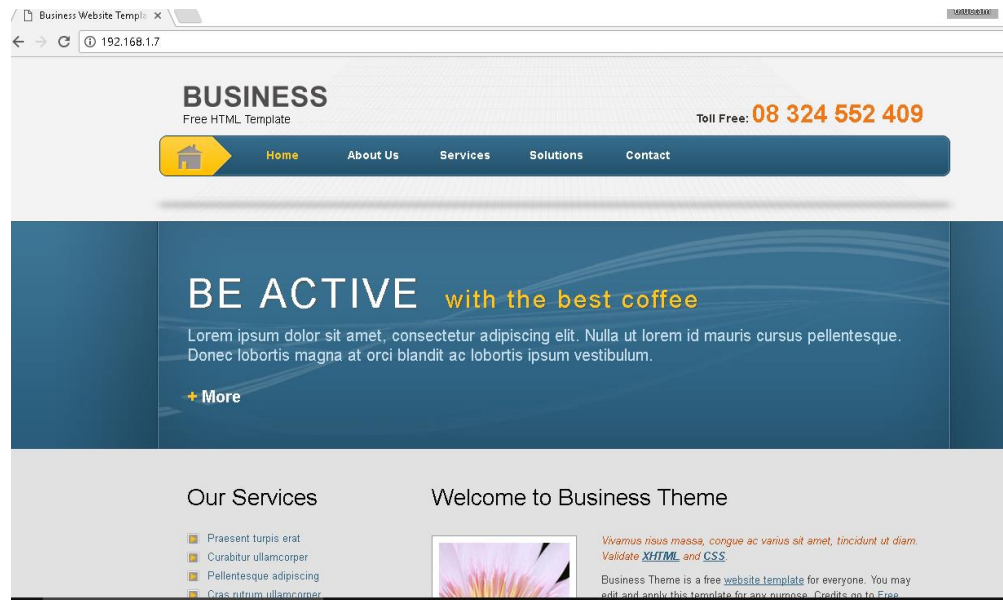
Truy cập <http://192.168.1.7>



Thay đổi trang mặc định của apache

Bước 4: download template website và copy vào thư mục /var/www/html

Bước 5: Truy cập <http://192.168.1.7>

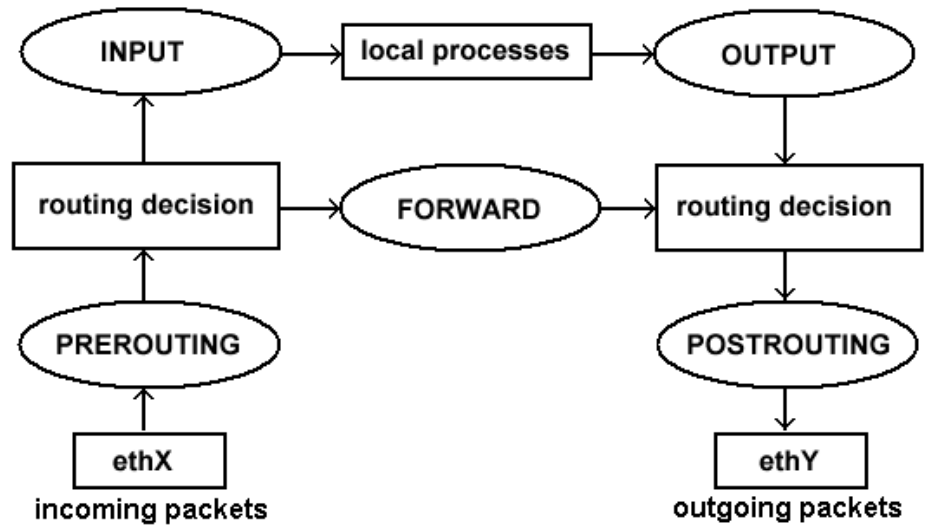


newstar

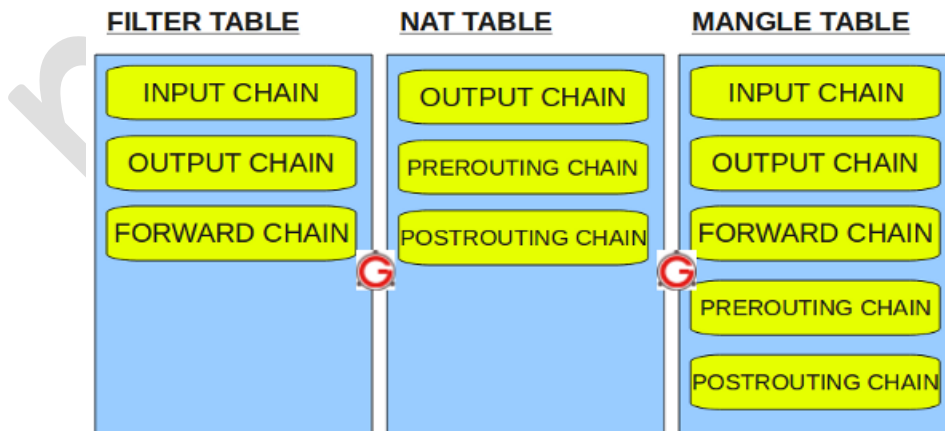
Chương 23: IPTABLES

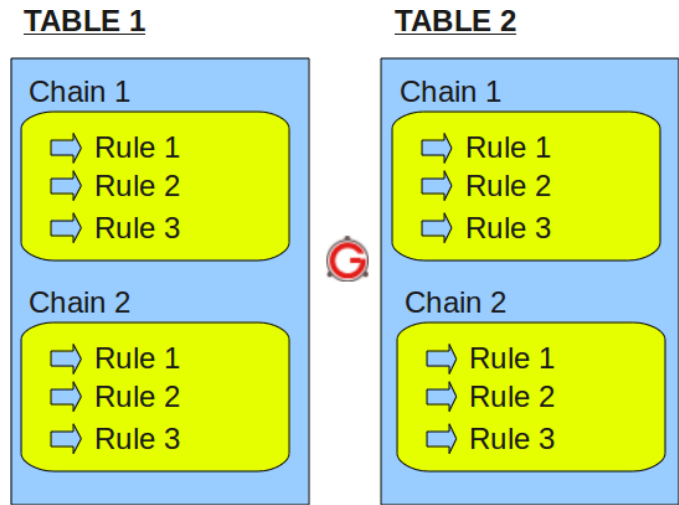
1) Giới thiệu

IPTABLES là hệ thống firewall tiêu chuẩn được tích hợp trong hầu hết hệ điều hành Linux. IPTABLES theo dõi luồng dữ liệu vào ra các interface, lọc gói dựa vào các thông tin của header tại các tầng của Data link, Network, Transport của mô hình OSI



Cấu trúc Iptables gồm 3 **Table**, mỗi table có các **Chain**, mỗi chain chứa các **Rule** do người quản trị cấu hình





- ✓ FILTER TABLE: dùng để lọc các gói tin, gồm các chain
 - INPUT: lọc những gói tin đi vào hệ thống
 - OUTPUT: lọc những gói tin đi ra từ hệ thống
 - FORWARD: Lọc gói dữ liệu đi đến các server khác kết nối trên các NIC khác của firewall
- ✓ NAT: sửa địa chỉ gói tin gồm các chain
 - PRE-ROUTING: Sửa địa chỉ đích của gói tin trước khi định tuyến
 - POST-ROUTING: Sửa địa chỉ nguồn của gói tin sau khi gói tin đã được định tuyến
 - OUTPUT: NAT địa chỉ local để đi ra ngoài.
- ✓ MANGLE: dùng để chỉnh sửa QOS bit trong phần TCP Header của gói tin

Gồm các chain: PREROUTING, OUTPUT, FORWARD, INPUT, POSTROUTING.

Cấu trúc tổng quát của rule

```
iptables [-t <table-name>] <command><chain-name> \ <parameter-1><option-1> \
<parameter-n><option-n>
```

Trong đó:

Iptables: là từ khóa bắt buộc phải có.

-t: là tùy chọn để chọn tên table sử dụng, thường kết hợp với <table-name>

Nếu không dùng tùy chọn `-t` thì mặc định iptables sẽ sử dụng Filter table

<command>:

-A	Nối 1 rule vào chain
-D	Xóa 1 rule ra khỏi chain
-I	Chèn 1 rule vào chain
-R	Thay thế rule
-L	Xem các rule đã được load
-N	Tạo một chain mới
-X	Xóa 1 chain
-E	Đổi tên chain

<chain-name>: lựa chọn các chain tương ứng với các table

<Parameters>:

PARAMETERS	Mô tả
-p	Protocol (tcp, udp, icmp)
-s	Source address [/mask]
-d	Destination address [/mask]
-i	Tên interface mà packet nhận vào
-o	Tên interface mà packet sẽ gửi ra

-j Chuyển packet đến target khi thỏa điều kiện của rule

Target có sẵn:

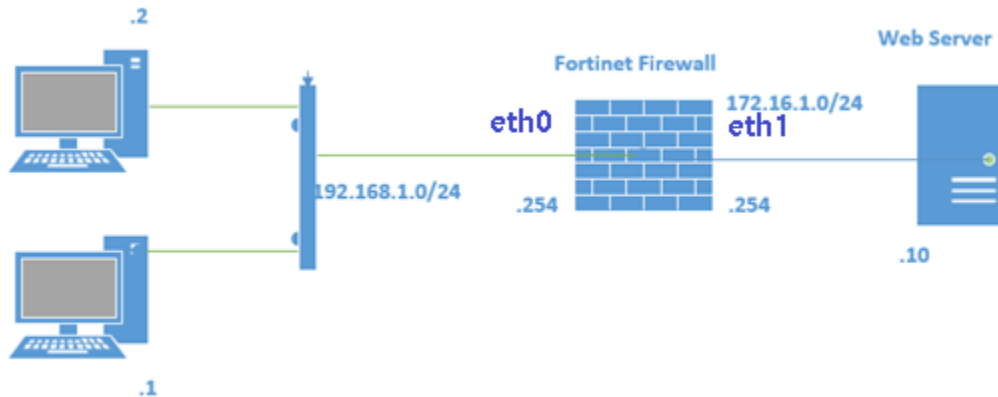
- **ACCEPT**: iptables chấp nhận chuyển data đến đích.
- **DROP**: iptables khóa những packet.
- **LOG**: thông tin của packet sẽ gửi vào syslog
 - **REJECT**: ngăn chặn packet và gửi thông báo cho sender
 - **DNAT**: thay đổi địa chỉ đích (--to-destination)
 - **SNAT**: Thay đổi địa chỉ source (--to-source)

<Options (match)>

parameters	Match options	Mô tả
-p tcp	--dport	Thiết lập destination port
	--sport	Thiết lập source port
	--syn	Gói TCP với cờ SYN bật lên
	--tcp-flags	thiết lập flags (SYN,ACK,FIN,RST)
-p udp	--dport	
	--sport	
-p icmp	-- icmp-type	Thiết lập loại icmp (echo-request, echo-reply, ...) #iptables -p icmp -h (để xem thêm)

-m multiport	--sport <port, port> --dport <port, port>	Lựa chọn nhiều port
---------------------	--	---------------------

2) Mô hình



3) Yêu cầu và cấu hình

- Cho phép tất cả client truy cập đến Server thông qua port 80
`#iptables -A FORWARD -i eth0 -d 172.16.1.10 -dport 80 -j ACCEPT`
- Chỉ phép PC 192.168.1.2 telnet đến Web Server
`#iptables -I FORWARD -I eth0 -s 192.168.1.2 -d 172.16.1.10 -dport 23 -j ACCEPT`