VERSION: 1.0

QUẢN TRỊ HỆ THỐNG LINUX – LPI II

BIÊN SOẠN: DƯƠNG VĂN TOÁN
EMAIL: DUONG.VAN.TOAN424@GMAIL.COM

MỤC LỤC

CHƯƠNG I: VNC SERVER

1) Giới Thiệu VNC SERVER

VNC – chữ viết tắt của Virtual Network Computing là một công cụ thông dụng và phổ biến để cung cấp cho người quản trị mạng có thể truy cập Server Linux từ xa thông qua giao diện đồ họa.

Trong bài viết này, chúng ta sẽ tiến hành cài đặt và cấu hình VNC Server trên Hệ Điều Hành Centos 6.5

2) Mô Hình Triển Khai

- ✓ **VNC Server – Centos 6.5:** 192.168.1.50/24
- ✓ **VNC Viewer (Client) – Windows:** 192.168.1.10/24

3) Cài Đặt VNC Server

❖ Bước 1: Cài đặt giao diện GNOME Desktop

Đôi khi chúng ta có thể cần đến giao diện GUI để thực hiện một số tác vụ trong Linux/Unix ngay cả khi những tác vụ đó không được ưu tiên cho quản trị Linux/Unix. Để tiến hành cài đặt giao diện GNOME Desktop trên HĐH Centos 6.5 chúng ta thực thi như sau:

*[root@localhost ~]# **yum groupinstall "Desktop"***

❖ Bước 2: Cài đặt TigerVNC-Server

*[root@localhost ~]# **yum –y install tigervnc-server***

❖ Bước 3: Cấu hình tài khoản truy cập VNC

- ➢ Sử dụng Tài khoản ***root*** để truy cập VNC bằng *vnc_ip_address:1* với đầy đủ quyền.
- ➢ Sử dụng Tài khoản ***toan*** để truy cập VNC bằng *vnc_ip_address:2*

_ Cài đặt mật khẩu khi truy cập VNC bằng tài khoản ***root:***

*[root@localhost ~]# **vncpasswd***

***Password**: 123456789*

***Verify**: 123456789*

_ Tạo mới tài khoản ***toan*** và cài đặt mật khẩu:

*[root@localhost ~]# **adduser toan***

[root@localhost ~]# passwd toan

_ Cài đặt mật khẩu khi truy cập VNC bằng tài khoản ***toan:***

*[root@localhost ~]# **su toan***

*[toan@localhost root]$ **vncpasswd***

***Password**: 123456789*

***Verify**: 123456789*

❖ Bước 4: Cấu hình VNC Server

➢ Cài đặt cấu hình truy cập VNC

_ Mở file /etc/sysconfig/vncservers. Cấu hình thêm những thông số sau vào cuối file:

*[root@localhost ~]# **vi /etc/sysconfig/vncservers***

VNCSERVERS=”1:root 2:toan” # Quy định tài khoản kết nối và port tương ứng.

VNCSERVERARGS[1]=”-geometry 1024x768” # Quy Định độ phân giải màn hình sau khi kết nối VNC

VNCSERVERARGS[2]=”-geometry 1024x768” # Quy Định độ phân giải màn hình sau khi kết nối VNC

➢ Tắt dịch vụ SELinux:

_ Để tắt dịch vụ này chúng ta dùng lệnh mở file cấu hình: *vi /etc/sysconfig/selinux*

_ Ở dòng **SELINUX=enforcing**, chúng ta chuyển thành **SELINUX=disabled**

_ Sau khi hoàn tất, chúng ta tiến hành khởi động lại máy.

- **Tắt dịch vụ Firewalld**

[root@localhost ~]# **/etc/rc.d/init.d/iptables stop:** ngừng dịch vụ iptables

[root@localhost ~]# **Chkconfig iptables off:** không cho dịch vụ iptables (IPv4) khởi động cùng hệ thống

[root@localhost ~]# **Chkconfig iptables off:** không cho dịch vụ iptables (IPv6) khởi động cùng hệ thống

_ Để kiểm tra trạng thái dịch vụ firewalld đã được tắt hay chưa, chúng ta sử dụng lệnh sau:

[root@localhost ~]# **Service iptables status:** Nếu có thông báo **Firewall is not running** – Chúng ta đã cài đặt tắt Firewall thành công.

- **Mở port truy cập VNC Server**

_ Chúng ta có thể tiến hành mở port truy cập trên VNC Server thay vì tắt firewall vì lý do bảo mật cho hệ thống Server Linix/Unix. Chúng ta có thể mở port 590X, với X là chỉ số port tương ứng của mỗi Tài khoản. Ví dụ ở đây là: 5901, 5902.

*[root@localhost ~]# **iptables –I INPUT –p tcp – dport 5901:5902 –j ACCEPT***

*[root@localhost ~]# **service iptables save:*** lưu cấu hình iptables

*[root@localhost ~]# **service iptables restart:*** khởi động lại dịch vụ iptables

- **Cấu hình VNC Server luôn khởi động cùng Server**

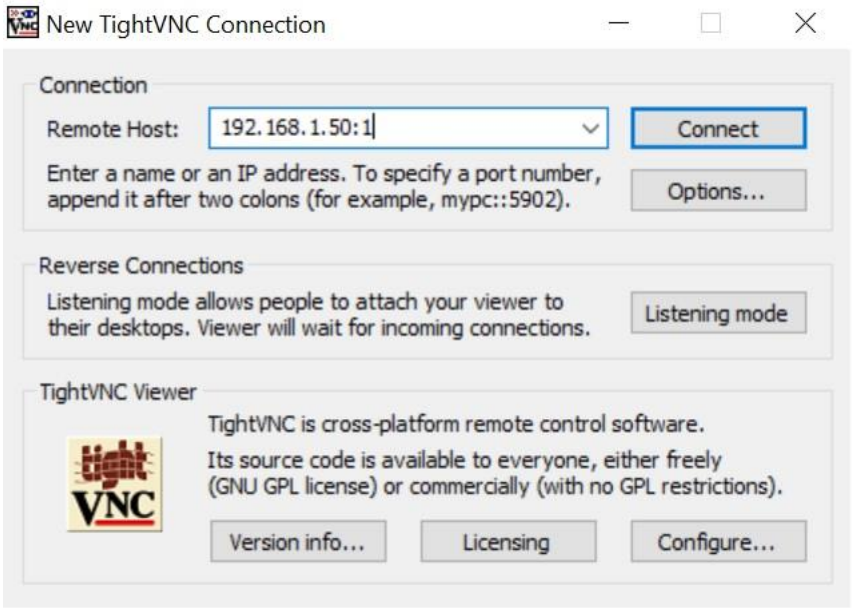
*[root@localhost ~]# **chkconfig vncserver on***

➢ Khởi động dịch vụ VNC Server

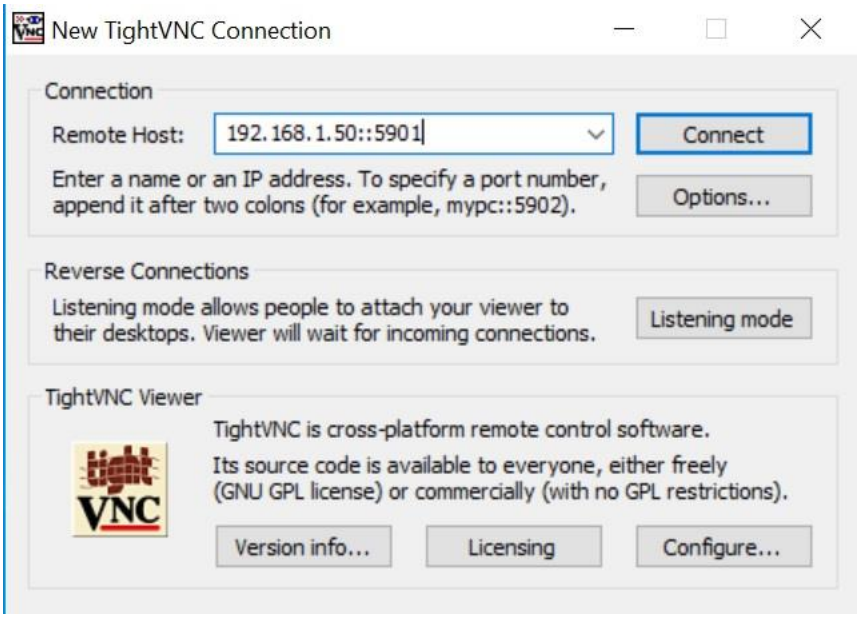
*[root@localhost ~]# **service vncserver start***

❖ Bước 5: Kết nối VNC Server

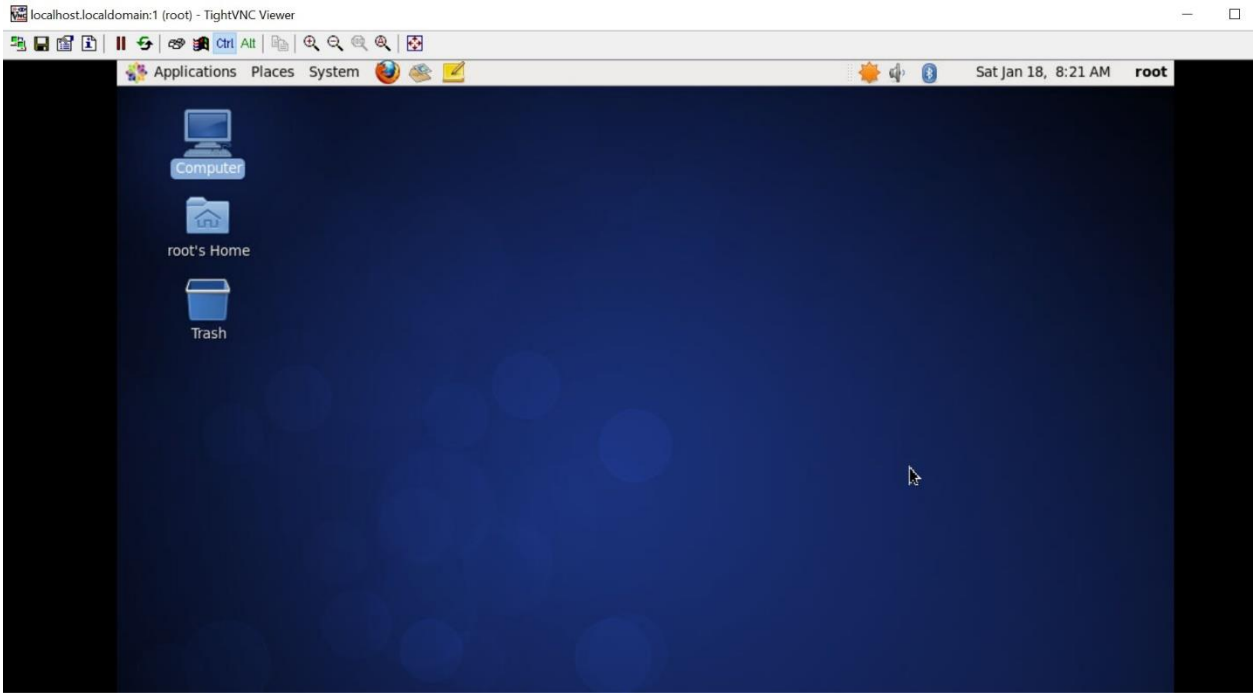
Chúng ta tiến hành cài đặt **TightVNC** cho **Windows** hoặc **VNC Viewer** của **RealVNC** (có hỗ trợ cho máy MAC), sau đó tiến hành chạy **VNC Viewer** để kết nối đến **VNC Server** bằng địa chỉ IP và Port VNC đã cài đặt. Ví dụ: 192.168.1.50:1 cho Tài khoản ***root*** và 192.168.1.50:2 cho Tài khoản ***toan*** (trong đó: 192.168.1.50 – là địa chỉ IP của **VNC Server**)



Hoặc



_ Sau khi truy cập thành công, chúng ta sẽ có giao diện như sau:



CHƯƠNG II: DHCP SERVER

1) Giới Thiệu DHCP SERVER

- **DHCP** - chữ viết tắt của 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 địa chỉ IP tĩnh. Thông tin mà các DHCP client nhận được từ DHCP server bao gồm: IP, subnet mask, default gateway, DNS server, …
- DHCP server được sử dụng để cấp phát các địa chỉ IP duy nhất và tự động gán cấu hình các thông tin khác cho các DHCP Client. Trong hầu hết các gia đình và các doanh nghiệp nhỏ, router hoặc modem hoạt động như DHCP server. Trong các mạng lớn, một máy chủ duy nhất có thể hoạt động như một DHCP server.

Quá trình cấp phát một địa chỉ IP từ DHCP Server cho các DHCP Client diễn ra như sau: Một thiết bị (client) yêu cầu một địa chỉ IP từ một router (hoặc máy chủ), sau đó Server sẽ gán một địa chỉ IP có sẵn chưa được cấp cho các Client khác để cho phép Client giao tiếp với mạng.

Khi một thiết bị đã được bật chế độ xin cấp địa chỉ IP bằng DHCP và kết nối với mạng có DHCP server, nó sẽ gửi một yêu cầu đến máy chủ này, được gọi là yêu cầu DHCPDISCOVER. Sau khi gói tin DISCOVER đến DHCP server, máy chủ sẽ cố gắng giữ một địa chỉ IP mà thiết bị có thể sử dụng, và sau đó cung cấp cho client địa chỉ này với một gói DHCPOFFER.

Sau khi cung cấp địa chỉ IP đã chọn, thiết bị đáp ứng với DHCP server bằng một gói tin DHCPREQUEST để chấp nhận nó, sau đó máy chủ gửi ACK được sử dụng để xác nhận thiết bị có địa chỉ IP cụ thể đó và để xác định khoảng thời gian mà thiết bị có thể sử dụng địa chỉ trước khi lấy địa chỉ mới. Nếu máy chủ quyết định rằng thiết bị không có địa chỉ IP, nó sẽ gửi một NACK. Tất nhiên điều này xảy ra rất nhanh và bạn không cần biết bất kỳ loại kỹ thuật nào được sử dụng để lấy địa chỉ IP từ DHCP server.

- **Các thành phần của DHCP**

Khi làm việc với DHCP, bạn cần hiểu tất cả thành phần của nó. Dưới đây là danh sách các thành phần của DHCP.

- ✓ **DHCP server:** Một thiết bị mạng chạy dịch vụ DHCP chứa địa chỉ IP và thông tin cấu hình liên quan. Đây thường là máy chủ hoặc router nhưng có thể là bất cứ thứ gì hoạt động như máy chủ chẳng hạn như thiết bị SD-WAN.

- ✓ **DHCP client**: Thiết bị nhận thông tin cấu hình từ máy chủ DHCP. Đây có thể máy tính, thiết bị di động, thiết bị IoT (Internet of Things) hoặc bất cứ thiết bị gì khác yêu cầu kết nối mạng. Hầu hết các thiết bị này được cấu hình để nhận thông tin DHCP theo mặc định.
- ✓ **IP address pool**: Dãy địa chỉ có sẵn cho client DHCP. Những địa chỉ này thường được truyền tuần tự từ thấp nhất đến cao nhất.
- ✓ **Subnet**: Mạng IP có thể được phân thành các phân đoạn được gọi là subnet (mạng con). Mạng con giúp mạng được quản lý dễ dàng hơn.
- ✓ **Lease**: Khoảng thời gian client DHCP giữ thông tin địa chỉ IP. Khi khoảng thời gian này hết hạn, client phải làm mới nó.
- ✓ **DHCP relay**: Router hoặc máy chủ nghe tin nhắn được phát trên mạng đó và sau đó chuyển chúng đến một máy chủ được cấu hình. Máy chủ này sau đó phản hồi lại relay agent để truyền chúng đến client. Nó được sử dụng để tập trung máy chủ DHCP thay vì để máy chủ trên mỗi mạng con.

2) Mô Hình Triển Khai

- ✓ **DHCP SERVER – Centos 6.5:** 192.168.1.50/24
- ✓ **DHCP Client – Windowns 10.**

3) Cài Đặt DHCP Server

❖ Bước 1: Cài đặt gói DHCP

- ➢ Trước khi tiến hành cài đặt DHCP Server, chúng ta cần cài đặt địa chỉ IP tĩnh cho DHCP Server là: 192.168.1.50/24 (Default Gateway: 192.168.1.1; DNS Server: 8.8.8.8). Địa chỉ của DHCP Server sẽ trùng với dải địa chỉ IP sẽ cấp cho các DHCP Client.

*[root@localhost ~]# **vi /etc/sysconfig/network-scripts/ifcfg-eth0***

DEVICE=”eth0”

HWADDR=”00:0C:29:F1:01:1B”

NM_CONTROLLED=”yes”

ONBOOT=”yes”

BOOTPROTO=”none”

IPADDR=192.168.1.50

NETMASK=255.255.255.0

GATEWAY=192.168.1.1

DNSSERVER=8.8.8.8

- Tiến hành cài đặt cập Repositories và các gói:

*[root@localhost ~]# **yum update***

- Cài đặt gói DHCP:

*[root@localhost ~]# **yum –y install dhcp***

❖ **Bước 2: Cấu hình dịch vụ DHCP**

- Mở file */etc/sysconfig/dhcpd* và thêm interface sẽ lắng nghe và phản hồi các gói tin DHCP từ các DHCP Client.

*[root@localhost ~]# **vi /etc/sysconfig/dhcpd***

DHCPDARGS=eth0

- Tiếp theo, chỉnh sửa các tham số cho DHCP Server trong file: */etc/dhcp/dhcpd.conf*

*[root@localhost ~]# **vi /etc/dhcp/dhcpd.conf***

Option domain-name “abc.com.vn”; # Tùy chọn cấp thêm tên miền khi cấp địa chỉ IP

Option domain-name-servers 8.8.8.8, 8.8.4.4; # Cấp địa chỉ DNS Server kèm theo khi cấp IP

Default-lease-time 600; # Thời gian mặc định để cấp mới lại một địa chỉ IP.

Max-lease-time 7200; # Thời gian tối đa để cấp mới lại một địa chỉ IP.

Log-facility local7; # Đặt phương pháp log là Local7 – log dự trữ cho sử dụng nội bộ.

Subnet 192.168.1.0 netmask 255.255.255.0 {

Range 192.168.1.100 192.168.100.254; # Dải địa chỉ IP sẽ được cấp phát.

Option broadcast-address 192.168.1.254; # Địa chỉ Broadcast của dải mạng.

Option routers 192.168.1.1; # Cấp phát địa chỉ Default Gateway.

}

Host PC_A {

Hardware Ethernet 02:12:34:45:ED:00;

Fixed-address 192.168.1.110;

Cấp động cố định địa chỉ IP: 192.168.1.110 cho PC_A có địa chỉ MAC trên.

}

- Bây giờ thực hiện việc khởi động dịch vụ DHCP

*[root@localhost ~]# **service dhcpd start***

- Cấu hình DHCP luôn khởi động cùng với Server.

*[root@localhost ~]# **chkconfig –levels 235 dhcpd on***

- Dưới đây là danh sách và ý nghĩa của mỗi Run Level:

0 Halt
1 Single-User mode
2 Multi-user mode console logins only (without networking)
3 Multi-User mode, console logins only
4 Not used/User-definable
5 Multi-User mode, with display manager as well as console logins (X11)
6 Reboot

- **Chúng ta có thể xem danh sách các địa chỉ IP đã được cấp phát cho các DHCP Client bằng:**

[root@localhost ~]# **cat /var/lib/dhcpd/dhcpd.leases**

CHƯƠNG III: SAMBA

1) Giới Thiệu SAMBA

- Máy chủ Samba được xem là một Máy chủ tập tin (File Server), sử dụng trong mạng nội bộ. Là nơi lưu trữ tập trung các thông tin của một tổ chức, doanh nghiệp bất kỳ và thường được cài đặt trên hệ điều hành Linux hoặc Windows. Máy chủ Samba hoạt động chủ yếu dựa trên giao thức SMB (Server Message Block Protocol) được công bố năm 1984 trong một tài liệu kỹ thuật của hãng IBM với mục đích ban đầu là thiết kế một giao thức mạng để đặt tên và duyệt (naming and browsing).

- Cách thức hoạt động sơ bộ của giao thức SMB

Đối với giao thức SMB (tên gọi sơ khai của CIFS), nó hoạt động trong mạng Internet dựa trên giao thức TCP/IP. Và đem đến cho người dùng toàn quyền trong việc tạo một tập tin với các quyền hạn như Chỉ đọc (Read Only), Đọc và ghi (Read-Write), đặt mật khẩu, khóa một tập tin, …. Ngoài ra, SMB còn hỗ trợ các tính năng khác như:

- ✓ Đàm phán, dàn xếp để tương thích giữa các trạng thái SMB
- ✓ Phát hiện các máy chủ sử dụng SMB trên mạng (browse network)
- ✓ Xác thực truy cập file, thư mục chia sẻ
- ✓ Thông báo sự thay đổi file và thư mục
- ✓ Xử lý các thuộc tính mở rộng của file
- ✓ Hỗ trợ Unicode

2) Mô Hình Triển Khai

- SamBa Server: CentOS 6.5
  - **Hostname:** sambaserver.abc.com
  - **IP Address:** 192.168.1.50/24
- SamBa Client: Windows 10
  - **Hostname:** Client
  - **IP Address:** 192.168.1.162/24

3) Cài Đặt Samba Server

❖ **Bước 1:** Cài đặt gói Samba

_ Kiểm tra và gỡ bỏ những phiên bản Samba đã cài đặt trước:

[root@sambaserver ~]# *rpm –qa | grep samba*

[root@sambaserver ~]# *yum list installed | grep samba*

_ Nếu Samba đã được cài đặt, hãy gỡ bỏ bằng cách sau:

[root@sambaserver ~]# *yum remove samba**

_ Bây giờ, tiến hành cài đặt mới gói Samba:

[root@sambaserver ~]# *yum install samba* -y*

❖ **Bước 2: Cấu hình một thư mục chia sẻ với đầy đủ quyền**

_ Tạo một thư mục tên là *'/samba/share1'* và cấu hình đầy đủ quyền cho thư mục đó:

[root@sambaserver ~]# *mkdir –p /samba/share1*

[root@sambaserver ~]# *chmod –R 0777 /samba/share1*

_ Sửa và thêm một số dòng sau vào file cấu hình của samba như bên dưới:

[root@sambaserver ~]# vi /etc/samba/smb.conf

Dòng số 58 – Thêm 2 dòng sau vào phía dưới dòng số 58

Unix charset = UTF-8

Dos charset = CP932

Dòng số 75 – Thay đổi Workgroup mặc định của Windows

Workgroup = WORKGROUP

Dòng số 81 – Bỏ comment và cấu hình dải địa chỉ IP được cho phép truy cập dịch vụ Samba

Hosts allow = 127. 192.168.1.

Dòng số 102 – Cấu hình xác thực cho Samba

Security = share

Thêm những dòng sau vào cuối file

[myshare]

Path = /samba/share1

Writable = yes

Browsable = yes

Guest ok = yes

Guest only = yes

Create mode = 0777

Directory mode = 0777

_ Khởi động dịch vụ Samba trên Server

[root@sambaserver ~]# */etc/init.d/smb start*

[root@sambaserver ~]# */etc/init.d/nmb start*

[root@sambaserver ~]# *chkconfig smb on*

[root@sambaserver ~]# *chkconfig nmb on*

❖ **Bước 3: Kiểm tra cấu hình của Samba Server**

Để kiểm tra cấu hình hoạt động của Samba Server sử dụng lệnh: ***testparm***

[root@sambaserver ~]# ***testparm***

```
Load smb config files from /etc/samba/smb.conf

rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

Processing section "[homes]"

Processing section "[printers]"

Processing section "[myshare]"

Loaded services file OK.

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

[global]

dos charset = CP932

server string = Samba Server Version %v

security = SHARE

log file = /var/log/samba/log.%m

max log size = 50

hosts allow = 127., 192.168.1.

cups options = raw

[homes]

comment = Home Directories

read only = No

browseable = No

[printers]
```

comment = All Printers

path = /var/spool/samba

printable = Yes

browseable = No

[myshare]

path = /samba/share1

read only = No

create mask = 0777

directory mask = 0777

guest only = Yes

guest ok = Yes

❖ Bước 4: Cấu hình cho phép dịch vụ Samba trên Firewall

_ Mở file */etc/sysconfig/iptables* và tiến hành cấu hình cho phép mở các port mà Samba hoạt động: UDP và TCP/137, UDP và TCP/138, UDP và TCP/139, UDP và TCP/445, UDP và TCP/901

[root@sambaserver ~]# *vi /etc/sysconfig/iptables*

-A INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 137 -j ACCEPT

-A INPUT -s 192.168.1.0/24 -m state --state NEW -p udp --dport 138 -j ACCEPT

-A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 139 -j ACCEPT

-A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 445 -j ACCEPT

-A INPUT -s 192.168.1.0/24 -m state --state NEW -p tcp --dport 901 -j ACCEPT

_ Khởi động lại dịch vụ firewall

[root@sambaserver ~]# *service iptables restart*

❖ Bước 5: Tắt dịch vụ SELINUX

[root@sambaserver ~]# *vi /etc/sysconfig/selinux*

This file controls the state of SELinux on the system.

SELINUX= can take one of these three values:

enforcing - SELinux security policy is enforced.

permissive - SELinux prints warnings instead of enforcing.

disabled - No SELinux policy is loaded.

SELINUX=disabled

SELINUXTYPE= can take one of these two values:

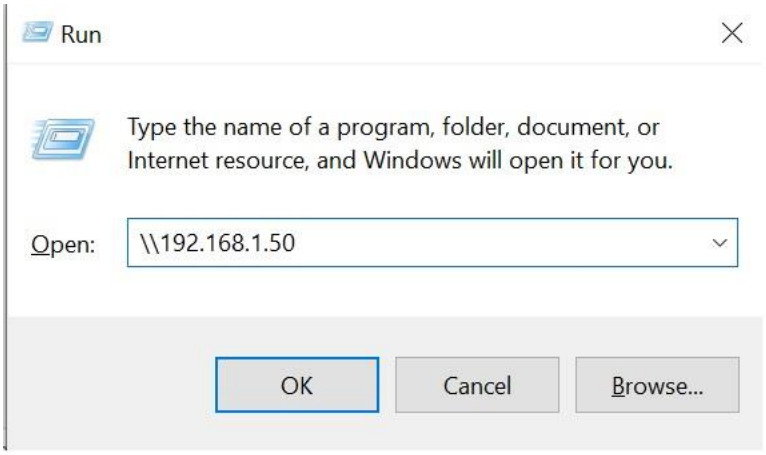
targeted - Targeted processes are protected,

mls - Multi Level Security protection.

SELINUXTYPE=targeted

_ Sau đó khởi động lại Samba Server.

❖ Bước 6: Test Samba Client (Windows)



❖ Bước 7: Tạo một thư mục chia sẻ trên Samba Server sử dụng xác thực

_ Tạo một tài khoản **"sk"** và tạo một nhóm **"smbgroup"**. Thêm tài khoản **"sk"** vào nhóm **"smbgroup"**

[root@sambaserver ~]# useradd sk

[root@sambaserver ~]# groupadd smbgroup

[root@sambaserver ~]# usermod -a -G smbgroup sk

[root@sambaserver ~]# smbpasswd -a sk

New SMB password: 123456789

Retype new SMB password: 123456789

_ Tạo một thư mục mới **"/samba/share2"** và gán quyền cho thư mục đó:

[root@sambaserver ~]# *mkdir /samba/share2*

[root@sambaserver ~]# *chmod -R 0755 /samba/share2/*

[root@sambaserver ~]# *chown -R sk:smbgroup /samba/share2/*

_ Thêm những dòng sau vào cuối file cấu hình Samba:

[root@sambaserver ~]# *vi /etc/samba/smb.conf*

[secure]

path = /samba/share2

writable = yes

browsable = yes

guest ok = no

valid users = @smbgroup

_ Khởi động lại dịch vụ Samba Server

[root@sambaserver ~]# */etc/init.d/smb restart*

[root@sambaserver ~]# */etc/init.d/nmb restart*

_ Test lại truy cập vào Samba Server sử dụng Client (Windows)

CHƯƠNG IV: NFS SERVER

1) GIỚI THIỆU NFS SERVER

NFS – chữ viết tắt của 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.

Hiện tại có 3 phiên bản NFS là NFSv2, NFSv3, NFSv4.

2) MÔ HÌNH TRIỂN KHAI NFS SERVER

- ✓ **Địa chỉ IP NFS Server:** 192.168.1.50/24
- ✓ **Địa chỉ IP NFS Client:** 192.168.1.162/24

3) CÀI ĐẶT NFS SERVER

❖ Bước 1: Cài đặt dịch vụ NFS trên Server

*[root@localhost ~]# **yum install nfs* -y***

❖ Bước 2: Khởi động dịch vụ NFS trên Server

*[root@localhost ~]# **service rpcbind start***

*[root@localhost ~]# **chkconfig rpcbind on***

*[root@localhost ~]# **service nfs start***

*[root@localhost ~]# **chkconfig nfs on***

❖ Bước 3: Cài đặt dịch vụ NFS trên Client

*[root@localhost ~]# **yum install nfs* -y***

❖ Bước 4: Khởi động dịch vụ NFS trên Client

*[root@localhost ~]# **service rpcbind start***

*[root@localhost ~]# **chkconfig rpcbind on***

*[root@localhost ~]# **service nfs start***

*[root@localhost ~]# **chkconfig nfs on***

❖ **Bước 5: Tạo thư mục chia sẻ trên Server**

_ Tạo thư mục chia sẻ tên **"/var/abc_share"** trên Server và cho phép người dung từ Client có thể đọc và ghi những file được tạo trên thư mục này.

*[root@localhost ~]# **mkdir /var/abc_share***

*[root@localhost ~]# **chmod 755 /var/abc_share***

❖ **Bước 6: Sửa thư mục đã chia sẻ trên NFS Server**

_ Sửa file */etc/exports,*

*[root@localhost ~]# **vi /etc/exports***

Thêm đoạn sau vào file

/var/abc_share/ 192.168.1.0/24(rw,sync,no_root_squash,no_all_squash)

Trong đó:

- ***/var/abc_share*** là thư mục đã được chia sẻ

- ***192.168.1.0/24*** là dải địa chỉ IP của Clients

- ***rw*** là quyền ghi trên thư mục được chia sẻ

- ***sync*** cho phép đồng bộ thư mục được chia sẻ giữa NFS Server và NFS Client

- ***no_root_squash*** cho phép tài khoản root được sử dụng xác thực khi truy cập thư mục chia sẻ

- ***no_all_squash*** cho phép xác thực đối với các tài khoản thường.

❖ **Bước 7: Khởi động dịch vụ NFS**

*[root@localhost ~]# **service nfs restart***

❖ **Bước 8: Mount thư mục chia sẻ trên Client**

_ Tạo một thư mục trên Client để mount thư mục đã chia sẻ trên NFS Server: "***/var/abc_share"*** đã tạo ở Bước 5:

[root@localhost ~]# ***mkdir /var/nfs_share***

_ Tiến hành mount thư mục chia sẻ từ NFS Server đến Client:

[root@localhost ~]# ***mount –t nfs 192.168.1.50:/var/abc_share/ /var/nfs_share/***

Mount.nfs: Connection timed out

-> Sau khi thực hiện lệnh mount, chúng ta sẽ thấy lỗi ***Connection timed out*** xuất hiện. Là do firewall đang chặn dịch vụ NFS trên Server. Để cho phép dịch vụ NFS được phép truy cập từ Client, chúng ta tiến hành mở các port của dịch vụ NFS trên Server.

[root@localhost ~]# ***vi /etc/sysconfig/iptables***

-A INPUT -m state --state NEW -m tcp -p tcp --dport 2049 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 111 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 32803 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 892 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 875 -j ACCEPT

-A INPUT -m state --state NEW -m tcp -p tcp --dport 662 -j ACCEPT

_ Khởi động lại dịch vụ Firewall

[root@localhost ~]# ***service iptables restart***

_ Thực hiện mount lại trên Client:

[root@localhost ~]# ***mount –t nfs 192.168.1.50:/var/abc_share/ /var/nfs_share/***

❖ Bước 9: Kiểm tra NFS

_ Kiểm tra thư mục chia sẻ trên NFS Server đã được mount trên Client chưa sử dụng lệnh ***"mount"***

[root@localhost ~]# ***mount***

/dev/mapper/vg_client-lv_root on / type ext4 (rw)

proc on /proc type proc (rw)

sysfs on /sys type sysfs (rw)

devpts on /dev/pts type devpts (rw,gid=5,mode=620)

tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")

/dev/sda1 on /boot type ext4 (rw)

none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)

sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)

nfsd on /proc/fs/nfsd type nfsd (rw)

192.168.1.50:/var/abc_share/ on /var/nfs_share type nfs

(rw,vers=4,addr=192.168.1.50,clientaddr=192.168.1.162)

CHƯƠNG V: WEB ADMIN

1) Giới Thiệu Web Admin

- ✓ **Webmin** là phần mềm quản trị server linux thông qua giao diện đồ họa. Cho phép người quản trị dễ dàng quản lý tài nguyên và cấu hình các dịch vụ thông qua dao diện web như: User management, Disk managemet, Network, Iptables (Firewall), Cron, Apache, DNS, Cronjob, CSDL MySQL…
- ✓ **Webmin** không thực sự mạnh mẽ như các Control Panel khác là cPanel, Direct Admin, … nhưng đây là một phần mềm miễn phí.
- ✓ **Webmin** sử dụng Port 10000 để giao tiếp.

2) Mô Hình Triển Khai

- ✓ **Webmin Server – CentOS 6.5:** 192.168.1.50/24
- ✓ **Windows 10 - Client:** 192.168.1.162/24

3) Cài Đặt Webmin

❖ **Bước 1: Cập nhật các Package của Hệ thống**

*[root@localhost ~]# **yum update –y***

❖ **Bước 2: Cài đặt Webmin thông qua Webmin Repo**

_ Tạo một file mới tên **webmin.repo** trong thư mục **/etc/yum.repos.d/** và nhập đoạn vào code như bên dưới:

*[root@localhost ~]# **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
```

_ Import PGP Key của Webmin:

*[root@localhost ~]# **rpm --import http://www.webmin.com/jcameron-key.asc***

_ Cài đặt Webmin và các gói phụ thuộc:

*[root@localhost ~]# **yum install webmin***

❖ Bước 3: Khởi động dịch vụ Webmin

*[root@localhost ~]# **service webmin start***

*[root@localhost ~]# **chkconfig webmin on***

_ Kiểm tra dịch vụ Webmin có đang chạy hay không:

*[root@localhost ~]# **service webmin status***

Webmin (pid 17049) is running

_ Dịch vụ Webmin sử dụng port 10 000

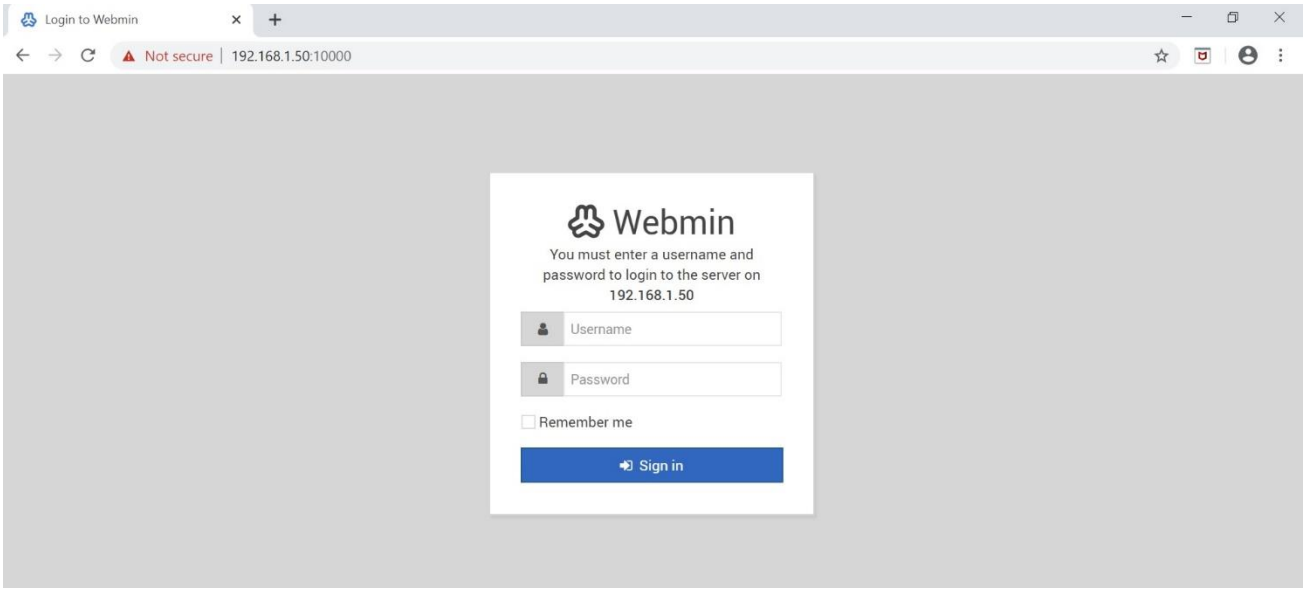
*[root@localhost ~]# **netstat –ta | grep 10000***

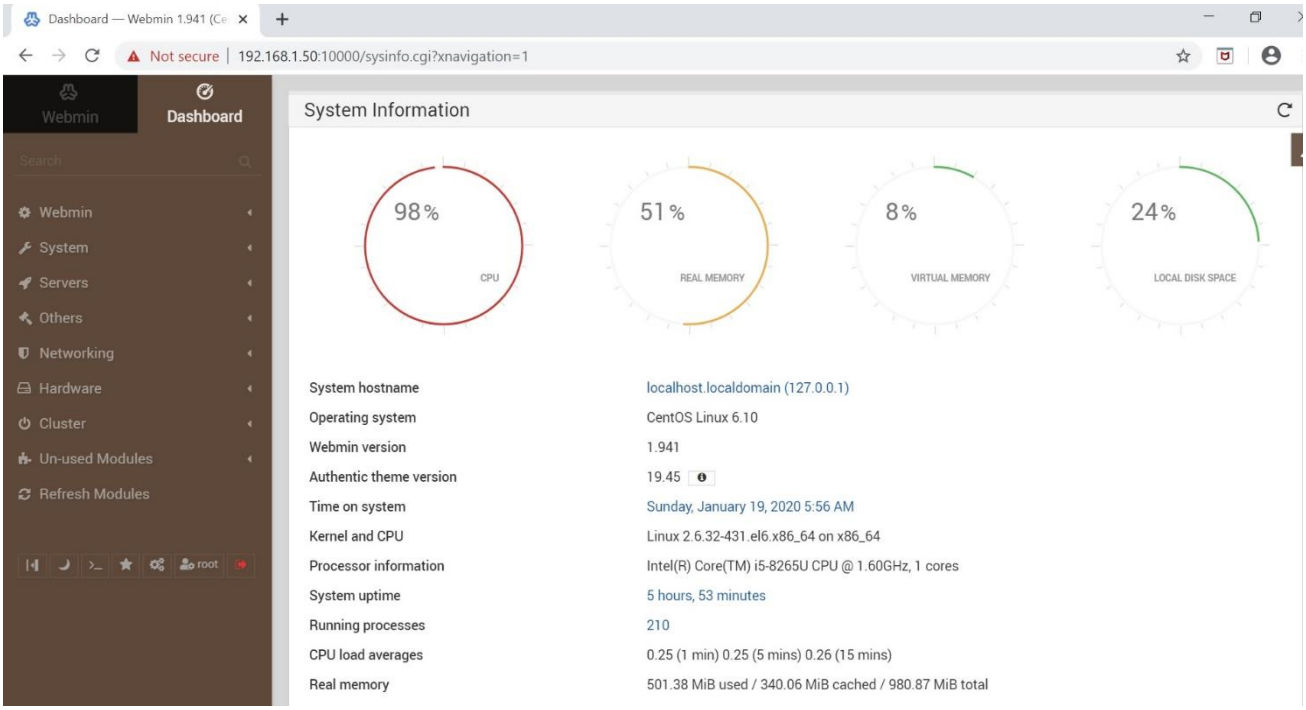
tcp 0 0 0.0.0.0:10000 0.0.0.0:* LISTEN 17049/perl

udp 0 0 0.0.0.0:10000 0.0.0.0:* 17049/perl

❖ Bước 4: Truy cập giao diện Webmin

https://địa_chỉ_ip_webminserver:10000




Dashboard — Webmin 1.941 (Ce
Not secure | 192.168.1.50:10000/sysinfo.cgi?xnavigation=1
Webmin
Dashboard
Search
Webmin
System
Servers
Others
Networking
Hardware
Cluster
Un-used Modules
Refresh Modules
root
System Information
98%
CPU
51%
REAL MEMORY
8%
VIRTUAL MEMORY
24%
LOCAL DISK SPACE
System hostname
localhost.localdomain (127.0.0.1)
Operating system
CentOS Linux 6.10
Webmin version
1.941
Authentic theme version
19.45
Time on system
Sunday, January 19, 2020 5:56 AM
Kernel and CPU
Linux 2.6.32-431.el6.x86_64 on x86_64
Processor information
Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz, 1 cores
System uptime
5 hours, 53 minutes
Running processes
210
CPU load averages
0.25 (1 min) 0.25 (5 mins) 0.26 (15 mins)
Real memory
501.38 MiB used / 340.06 MiB cached / 980.87 MiB total

CHƯƠNG VI: APACHE HTTP SERVER

1) GIỚI THIỆU

APACHE là một máy chủ Web mã nguồn mở hỗ trợ nhiều platform. Nó có khả năng cung cấp đầy đủ các tính năng của một máy chủ Web bao gồm: CGI, SSL và các tên miền ảo.

APACHE server sử dụng port mặc định là 80.

2) MÔ HÌNH TRIỂN KHAI

- ✓ **Apache Web Server – CentOS 6.5:** 192.168.1.50/24
- ✓ **Client – Windows:** 192.168.1.162/24

3) CÀI ĐẶT APACHE HTTP SERVER

❖ **Bước 1: Cài đặt gói Httpd**

*[root@localhost ~]# **yum install httpd –y***

❖ **Bước 2: Khởi động dịch vụ Apache**

*[root@localhost ~]# **service httpd start***

*[root@localhost ~]# **chkconfig httpd on***

❖ **Bước 3: Cấu hình Firewall cho phép truy cập dịch vụ Apache**

_ Mặc định Apache sử dụng port 80, vì vậy chúng ta cấu hình Firewall mở port 80

*[root@localhost ~]# **vi /etc/sysconfig/iptables***

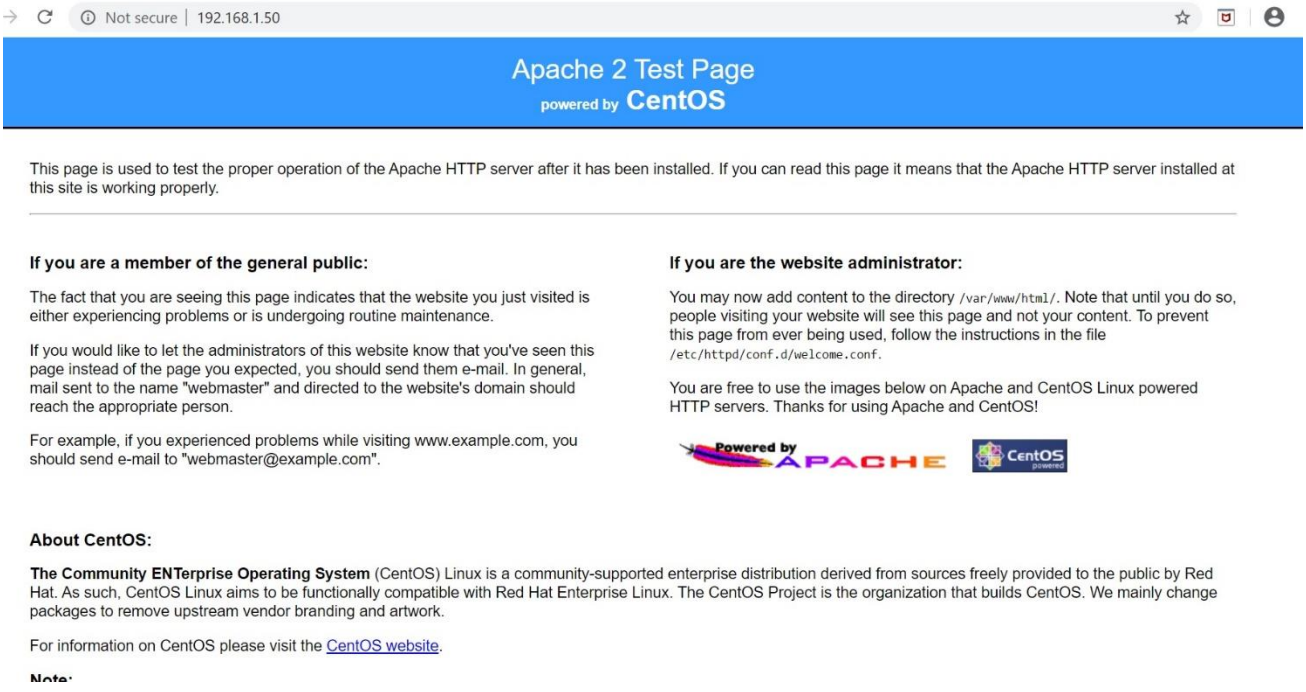
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT

_ Khởi động lại dịch vụ Firewall

*[root@localhost ~]# **service iptables restart***

❖ Bước 4: Kiểm tra Apache

_ http://192.168.1.50



❖ Bước 5: Tạo một Web Site đơn giản

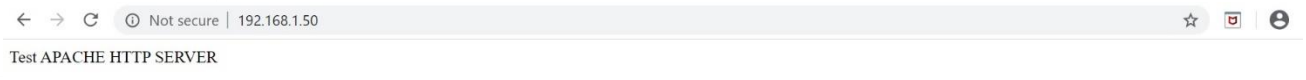
_ Tạo file ***index.html*** trong thư mục mặc định của Apache là: ***/var/www/html/***

*[root@localhost ~]# **cd /var/www/html***

*[root@localhost html]# **vi index.html***

<p1> Test APACHE HTTP SERVER </p1>

_ Bây giờ chúng ta có thể truy cập lại Apache Server: http://192.168.1.50 sẽ có kết quả như sau:



Test APACHE HTTP SERVER

CHƯƠNG VII: SQUID PROXY

1) GIỚI THIỆU

- ✓ Một **proxy server** là thiết bị có vai trò đứng giữa client và đích đến mà người dùng muốn truy cập. Proxy server cung cấp khả năng bảo mật, và thậm chí bảo vệ người dùng đứng sau Proxy. Ở các hệ điều hành **Red Hat, CentOS**, giải pháp **squid proxy** được nhiều người sử dụng vì tính an toàn, mạnh mẽ và linh hoạt.

- ✓ **Squid proxy** sẽ đứng giữa User và web server mà người dùng đang cố gắng kết nối đến. Sau nhiều lần thiết bị của bạn kết nối đến web server, Squid proxy sẽ thực hiện cache data và lưu trữ nội bộ để giảm thiểu thời gian tải trang, giảm thiểu băng thông và tác vụ phải xử lý lên các thiết bị firewall hoặc gateway.

- ✓ Một **Squid proxy server** thường là một server được cài đặt riêng biệt, tách biệt hoàn toàn so với Web server. Server sẽ hoạt động bằng cách theo dõi các đối tượng sử dụng lưu lượng mạng trong một network. Ban đầu, Squid sẽ đóng vai trò như là một thiết bị trung gian, đơn giản cho phép các request từ hướng client đi vào server và lưu lại một bản copy của request này. Sau đó nếu có phát sinh request tương tự từ user cũ hoặc các user mới request đúng bản copy này, Squid có thể ngay lập tức thay thế web server phản hồi user nhờ vào cache date, giúp tăng tốc độ download, giảm thiểu băng thông trên lưu lượng mạng.

2) MÔ HÌNH TRIỂN KHAI

- ✓ **Squid Proxy – CentOS 6.5:**
  - **Card Eth0:** 192.168.1.50/24 (Gateway: 192.168.1.1) – Kết nối Internet
  - **Card Eth1:** 172.16.1.1/24 – Kết nối vào mạng Lan
- ✓ **Client (Windows 10 hoặc CentOS):** 172.16.1.10/24 (Gateway: 172.16.1.1)

3) CÀI ĐẶT VÀ CẤU HÌNH SQUID PROXY

3.1. CÀI ĐẶT SQUID PROXY

_ Trước khi tiến hành cài đặt Squid Proxy trên Hệ Điều Hành CentOS 6.5, chúng ta thực hiện cập nhật các gói phần mềm của hệ điều hành hiện tại đang chạy:

[root@localhost ~]# *yum update –y*

_ Bây giờ chúng ta sẽ thực hiện việc cài đặt Squid Proxy theo các bước như bên dưới:

❖ **Bước 1: Cài đặt gói Squid và các gói phụ thuộc**

[root@localhost ~]# *yum install squid*

_ Theo mặc định, file cấu hình của Squid là: *"/etc/squid/squid.conf"* sẽ chứa cấu hình tối thiểu khuyến nghị của nhà phát triển phần mềm và tính năng lưu trữ trên bộ nhớ đệm (caching) sẽ làm việc bình thường mà chưa cần đến sự thay đổi hay cấu hình nào khác. Cấu hình tối thiểu của Squid theo khuyến nghị của nhà phát triển phần mềm có thể tham khảo như hình bên dưới:

root@localhost:~

```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8     # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
-- INSERT --
```

root@localhost:~

```
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

# Add any of your own refresh_pattern entries above these.
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320
-- INSERT --
```

❖ Bước 2: Khởi động dịch vụ Squid

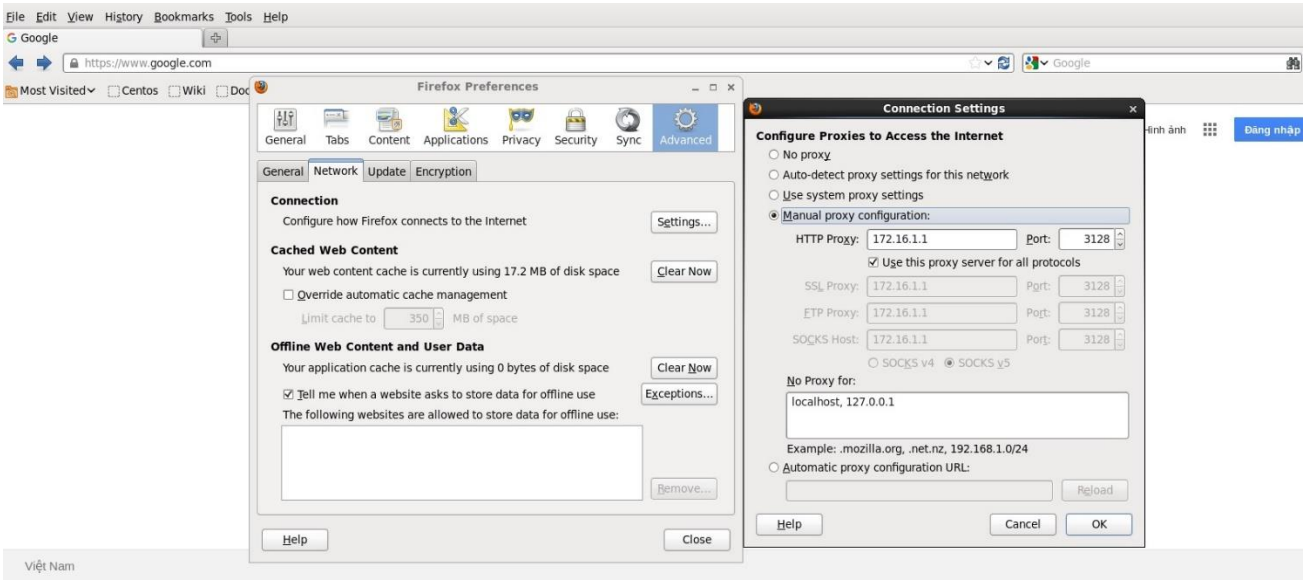
[root@localhost ~]# *service squid start*

[root@localhost ~]# *chkconfig –levels 235 squid on* *(#Cấu hình khởi động dịch vụ cùng hệ thống)*

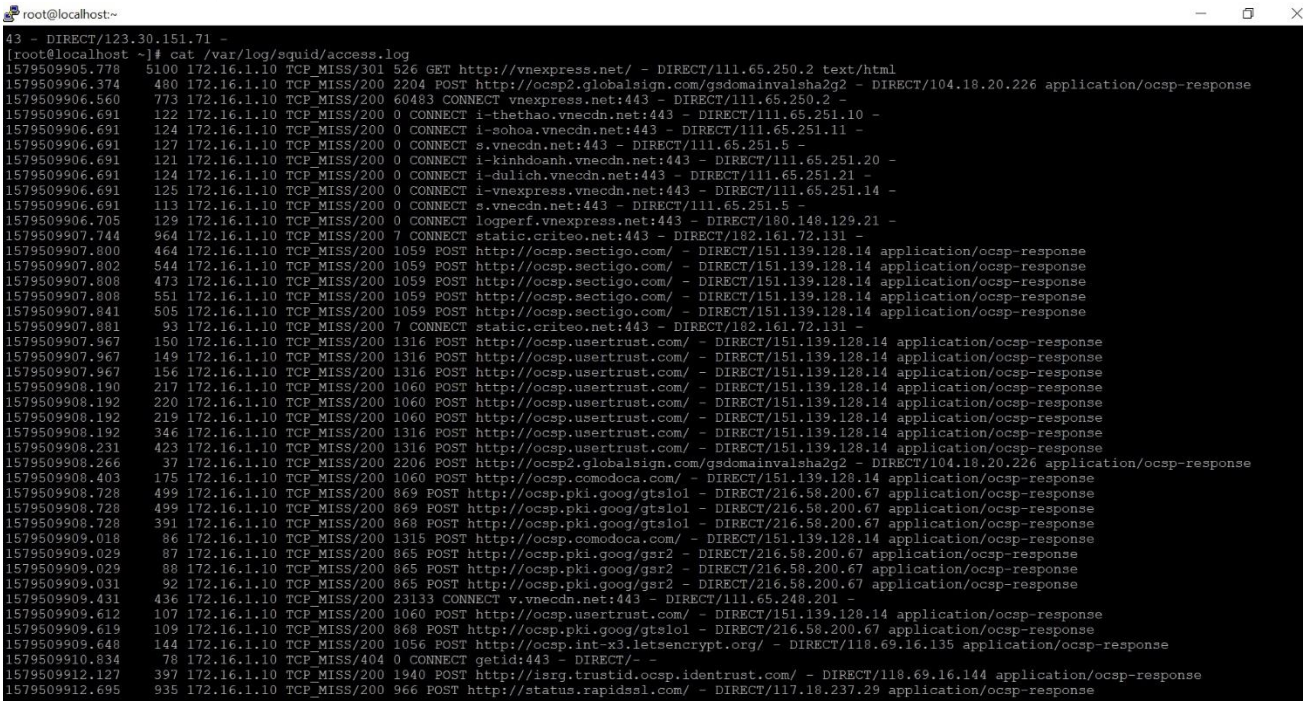
❖ Bước 3: Cài đặt trình duyệt Web trên Client truy cập Internet thông qua Proxy Server.

_ **IE:** Tools >> Internet Options >> Connections >> LAN Settings >> Chọn " Use a proxy server for your LAN" >> Nhập địa chỉ IP của Squid Proxy (172.16.1.1) và Port là 3128 (Đây là port mặc định của Squid Proxy)

_ **Firefox:** Options / Preferences >> Advanced >> Network >> Settings >> Chọn "Manual Proxy Configuration" >> Nhập địa chỉ IP của Squid Proxy (172.16.1.1) và Port là 3128 (Đây là port mặc định của Squid Proxy)



❖ Bước 4: Sử dụng trình duyệt trên Client truy cập vào 1 số trang web và kiểm tra log file trên Proxy



_ Trong trường hợp có lỗi xảy ra, không truy cập được Internet từ Client. Chúng ta tiến hành tắt Firewall và Selinux:

[root@localhost ~]# *service iptables stop*

[root@localhost ~]# *chkconfig iptables off*

[root@localhost ~]# *vi /etc/selinux/config*

SELINUX=disabled

_ Sau khi tắt Firewall và Selinux, chúng ta phải tiến hành khởi động lại Squid Proxy. Và thực hiện lại Bước 4.

3.2. CẤU HÌNH SQUID PROXY VỚI VAI TRÒ WEB FILTER (Lọc Web)

_ Chúng ta có thể hạn chế người dùng truy cập vào các trang Web hoặc các từ khóa bằng cách sử dụng Access Control Lists (ACLs).

3.2.1. Hạn chế truy cập vào các trang Web

❖ **Bước 1: Tạo một file chứa danh sách các trang web bị chặn**

_ Tạo một file mới **/etc/squid/blockedsites.squid** và nhập các trang web cần chặn vào file này:

[root@localhost ~]# *vi /etc/squid/blockedsites.squid*

#blocked sites

www.facebook.com

www.dantri.com.vn

www.vnexpress.net

❖ **Bước 2: Sửa file cấu hình Squid**

_ Mở file cấu hình của Squid: **/etc/squid/squid.conf** và tạo một ACLs mới tên là **"blocksites"** trong phần ACLs

[root@localhost ~]# *vi /etc/squid/squid.conf*

acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
ACL blocksites
acl blocksites dstdomain "/etc/squid/blockedsites.squid"

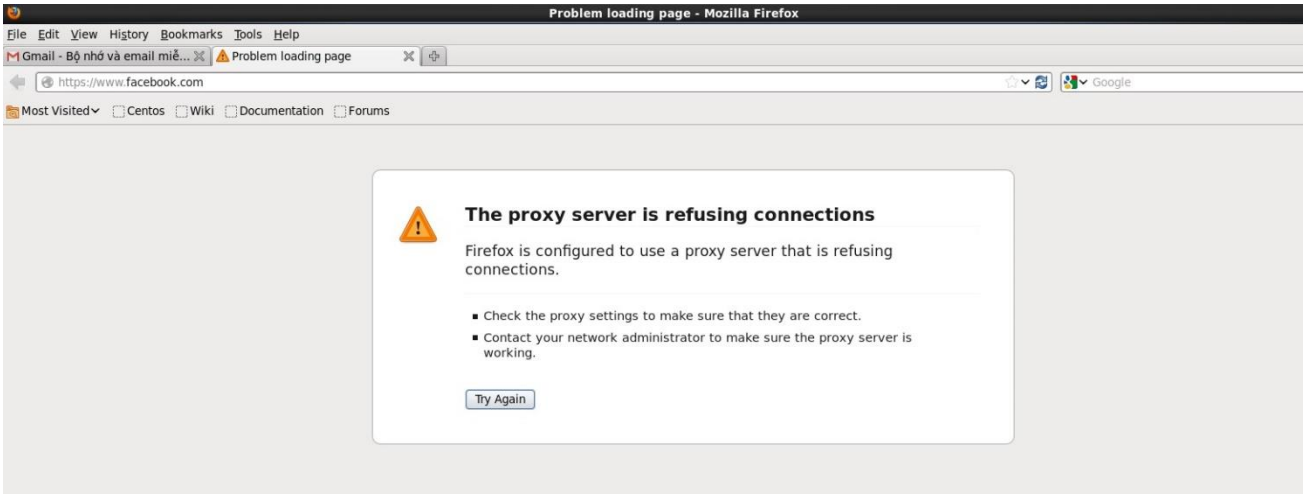
_ Sau đó thêm dòng **"http_access deny blocksites"** vào sau phần http: **"http_section"** để chặn truy cập từ các trang web trong danh sách "**blocksites**"

Only allow cachemgr access from localhost
http_access allow manager localhost
Deny access to blocksites ACL
http_access deny blocksites

❖ Bước 3: Khởi động lại dịch vụ Squid

[root@localhost ~]# *service squid restart*

Bước 4: Sử dụng trình duyệt Web của Client truy cập vào facebook.com.



_ Sau đó kiểm tra file Log trên Proxy, chúng ta sẽ thấy các yêu cầu đã bị chặn.

```
1579511187.367      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511189.465      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511189.755      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511190.087      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511190.725      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511191.429      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511191.911      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511204.236      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511204.418      1 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511204.589      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511204.767      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511204.948      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511205.154      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511205.896      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.083      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.256      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.412      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.564      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.734      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
1579511206.902      0 172.16.1.10 TCP_DENIED/403 3638 CONNECT www.facebook.com:443 - NONE/- text/html
```

3.2.2. Hạn chế truy cập bằng các từ Khóa

❖ Bước 1: Tạo một file với danh sách các từ khóa cần chặn

[root@localhost ~]# *vi /etc/squid/blockkeywords.squid*

#blocked keywords

Sex

Porn

Xxx

Phimcam

❖ **Bước 2: Sửa file cấu hình Squid**

_ Mở file cấu hình của Squid: **"/etc/squid/squid.conf"** và tạo mới một ACL tên **"blockkeywords"** và loại ACL là **"url_regex"** trong phần ACL

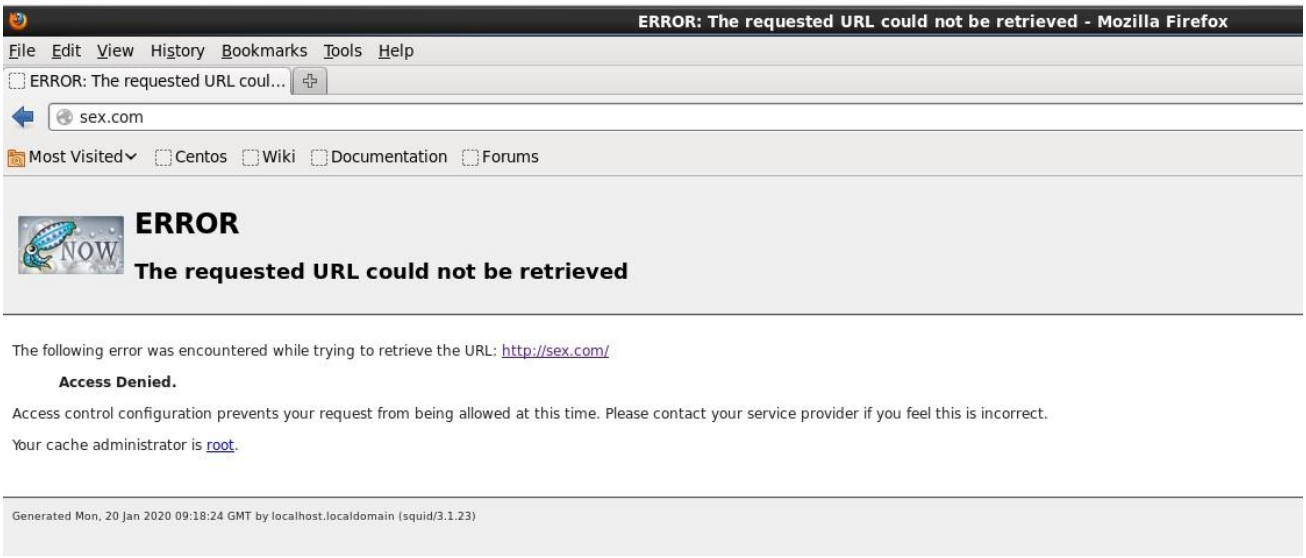
[root@localhost ~]# *vi /etc/squid/squid.conf*

```
acl Safe_ports port 488        # gss-http
acl Safe_ports port 591        # filemaker
acl Safe_ports port 777        # multiling http
acl CONNECT method CONNECT
# ACL blocksites
acl blocksites dstdomain "/etc/squid/blockedsites.squid"
# ACL blockkeywords
acl blockkeywords url_regex -i "/etc/squid/blockkeywords.squid"
```

_ Sau đó thêm dòng: **"http_access deny blockkeywords"** vào phần **"http_section"** để chặn truy cập vào các từ khóa có trong danh sách đã tạo.

```
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blocksites ACL
http_access deny blocksites
# Deny access to blockkeywords ACL
http_access deny blockkeywords
```

❖ **Bước 3: Sử dụng trình duyệt của Client truy cập**



_ Và xem File Log trên Proxy

```
1579511875.848 121635 172.16.1.10 TCP_MISS/200 5117 CONNECT id.google.com:443 - DIRECT/216.58.221.227 -
1579511886.850 136613 172.16.1.10 TCP_MISS/200 240820 CONNECT www.google.com:443 - DIRECT/216.58.221.228 -
1579511904.845      2 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579511905.515    588 172.16.1.10 TCP_MISS/200 13106 GET http://www.squid-cache.org/Artwork/SN.png - DIRECT/216.92.2.1
1579511905.538      0 172.16.1.10 TCP_DENIED/403 3823 GET http://sex.com/favicon.ico - NONE/- text/html
1579511994.657    428 172.16.1.10 TCP_MISS/403 1395 POST http://safebrowsing.clients.google.com/safebrowsing/downloads
1579512028.825      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512031.462      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512032.267      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512033.284      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512034.027      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512034.667      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512035.331      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512035.987      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512036.712      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512037.313      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512037.922      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512038.566      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512039.223      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512039.888      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512040.562      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
1579512041.121      0 172.16.1.10 TCP_DENIED/403 3790 GET http://sex.com/ - NONE/- text/html
```

3.2.3. Hạn chế truy cập đối với địa chỉ IP

Bước 1: Tạo danh sách địa chỉ IP sẽ bị chặn

_ Tạo một file mới **/etc/squid/blockip.squid** và thêm các địa chỉ IP cần chặn vào file này.

[root@localhost ~]# *vi /etc/squid/blockip.squid*

#blocked ips

172.16.1.20

172.16.1.21

Bước 2: Sửa file cấu hình Squid

_ Mở file **/etc/squid/squid.conf** và tạo một ACL mới tên **"blockip"** và loại ACL là **"src"** trong phần ACL

[root@localhost ~]# *vi /etc/squid/squid.conf*

```
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
# ACL blocksites
acl blocksites dstdomain "/etc/squid/blockedsites.squid"
# ACL blockkeywords
acl blockkeywords url_regex -i "/etc/squid/blockkeywords.squid"
# ACL blockip
acl blockip src "/etc/squid/blockip.squid"
```

_ Sau đó thêm dòng **"http_access deny blockip"** vào phần **"http_section"** để chặn truy cập Internet từ những IP nằm trong danh sách đã tạo

```
# Only allow cachemgr access from localhost
http_access allow manager localhost
# Deny access to blockip ACL
http_access deny blockip
# Deny access to blocksites ACL
http_access deny blocksites
# Deny access to blockkeywords ACL
http_access deny blockkeywords
```

3.3. Thay đổi Port hoạt động của Squid Proxy

_ Theo mặc định, Port hoạt động của Squid Proxy là 3128. Chúng ta có thể đổi port đó sang một port khác.

_ Mở file cấu hình Squid Proxy: **/etc/squid/squid.conf**

[root@localhost ~]# *vi /etc/squid/squid.conf*

http_port 8080 # Chỉ số port mới mà bạn muốn đổi

3.4. Hạn chế dung lượng Download

_ Chúng ta có thể hạn chế dung lượng download bằng cách sử dụng **reply_body_max_size**

_ Tiến hành thêm đoạn lệnh sau vào phần **http_access**

#Restrict download size

reply_body_max_size 10 MB all

CHƯƠNG VIII: IPTABLES

1) GIỚI THIỆU

❖ **IPTABLES** là một tiện ích tường lửa cực kỳ linh hoạt được xây dựng cho các hệ điều hành Linux. Iptables giám sát lưu lượng ra vào server bằng các rule được cấu hình. Khi một kết nối cố gắng tự thiết lập trên hệ thống của bạn, iptables sẽ tìm một quy tắc trong danh sách của nó để khớp với nó. Nếu không tìm thấy bất kì quy tắc nào có sẵn, thì sẽ áp dụng các rule mặc định với các gói tin

❖ Cấu trúc Iptables gồm 3 **Table: Filter Table, NAT Table, Mangle 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

_ IPtables có 3 hành động đối với một gói tin:

✓ ACCEPT: cho phép kết nối

✓ DROP: kết nối sẽ bị chặn và không có bất kì phản hồi nào cho server gửi đến. Thường được áp dụng cho các IP có hành động tấn công server. Cho các server đó biết là IP này không phản hồi như các IP không tồn tại.

✓ REJECT: Không cho phép kết nối, nhưng phản hồi lại lỗi. Điều này là tốt nhất nếu bạn không muốn một nguồn cụ thể kết nối với hệ thống của mình, nhưng bạn muốn họ biết rằng tường lửa của bạn đã chặn họ.

➢ 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.

2) MÔ HÌNH TRIỂN KHAI

✓ **CentOS 6.5:** Cài dịch vụ IPtables

3) CÀI ĐẶT VÀ CẤU HÌNH IPTABLES

3.1. IPTables InitScript

_ **IPTables** là một loại dịch vụ, cũng được quản lý tương tự như các dịch vụ khác trên Hệ Điều Hành Linux CentOS 6. Như chúng ta đã biết, **initsript** được sử dụng để quản lý dịch vụ iptables sẽ có khả năng: start, stop, reload …. Và không thể tự cấu hình được chính nó.

_ **IPTables initscript** được nằm trong **/etc/init.d/iptables (**ip6tables sử dụng cho phiên bản IPv6) và có thể sử dụng được hầu hết các tính năng thông thường như: start, stop, reload, restart, condrestart, status, panic và save.

- ✓ **/etc/init.d/iptables start**

Start là lệnh được sử dụng để khởi động (bật) dịch vụ iptables. Bạn cần cẩn thận và kiểm tra kỹ các luật nằm trong file **/etc/sysconfig/iptables** trước khi tiến hành khởi động dịch vụ iptables vì điều này có thể dẫn đến chặn một số dịch vụ mà bạn không mong muốn.

- ✓ **/etc/init.d/iptables stop**

Stop là lệnh được sử dụng để tạm dừng dịch vụ iptables. Khi bạn tiến hành tạm dừng dịch vụ iptables, có nghĩa là không có bất cứ luật nào của tường lửa được áp dụng và máy chủ sẽ có thể truy cập được trên tất cả các cổng đang chạy.

- ✓ **/etc/init.d/iptables reload**

Reload là lệnh được sử dụng để khởi động lại cấu hình hiện tại của dịch vụ iptables từ file **/etc/sysconfig/iptables.**

- ✓ **/etc/init.d/iptables condrestart**

Condrestart là lệnh được sử dụng để khởi động lại dịch vụ iptables nếu như dịch vụ đang chạy.

- ✓ **/etc/init.d/iptables status**

Status là lệnh được sử dụng để xem trạng thái hiện tại của các luật đang chạy. Bao gồm cả các luật được thêm vào thủ công của quản trị mạng và cả các luật có sẵn mặc định của dịch vụ iptables.

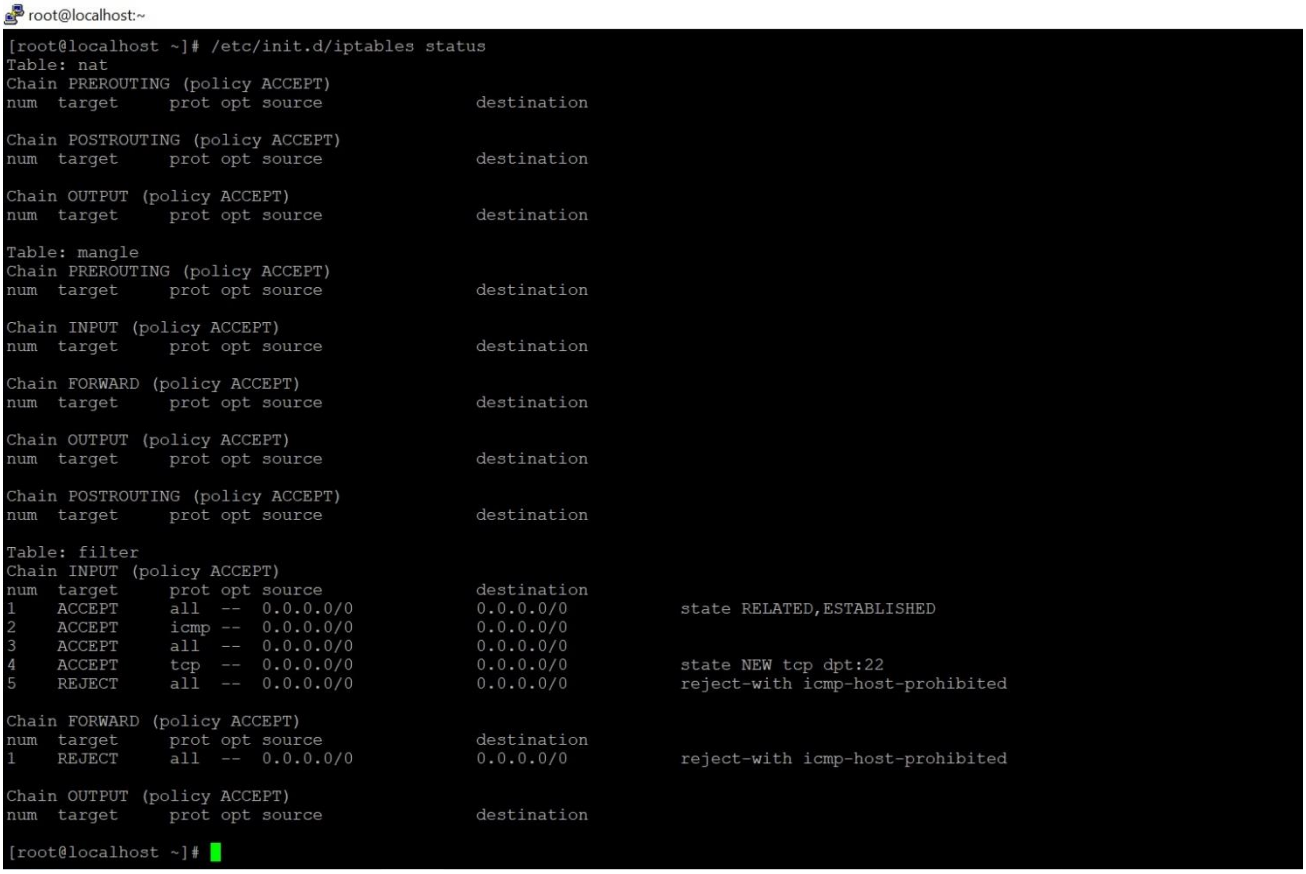
- ✓ **/etc/init.d/iptables panic**

Panic là lệnh được sử dụng để cấu hình tất cả các Chains của IPtables về trạng thái Drop. Lệnh Panic được sử dụng khi máy chủ đang trong tình trạng bị tấn công. Khi lệnh Panic được sử dụng thì toàn bộ các gói tin đến sẽ bị Drop, và sẽ Drop luôn cả kết nối SSH của bạn đến máy chủ.

- ✓ /etc/init.d/iptables save

Save là lệnh được sử dụng để lưu lại cấu hình đang chạy của iptables vào file cấu hình /etc/sysconfig/iptables,

_ Hình bên dưới là cấu hình mặc định của IPtables trên Hệ Điều Hành Linux CentOS 6:



3.2. Cấu hình Luật cho IPtables (Theo cách không tự lưu cấu hình)

_ Chúng ta sẽ cùng nghiên cứu về cách thêm hoặc xóa các luật mới vào IPtables theo phương pháp thủ công (manually). Có thể, từ thủ công không phải là từ thích hợp để miêu tả về những điều này. Nhưng dù sao đi nữa, chúng ta hãy cùng xem cách cấu hình các luật mới vào IPtables theo phương pháp này bằng cách sử dụng lệnh /sbin/iptables

_ Cú pháp sẽ được thực hiện như sau bằng các ví dụ dưới đây:

3.2.1. Cho phép lưu lượng HTTP (Sử dụng TCP Port 80)

[root@localhost ~]# *iptables –A INPUT –p tcp –m state –state NEW –m tcp –dport 80 –j ACCEPT*

_ Trong đó:

- ✓ -A: Append – chèn luật vào chuỗi INPUT (chèn xuống cuối).
- ✓ -p: Protocol – giao thức TCP, UDP hoặc ICMP
- ✓ -m –state: Kiểm tra trạng thái kết nối:
  - ESTABLISHED: trạng thái đã thiết lập kết nối
  - NEW: Bắt đầu thiết lập kết nối
  - RELATED: thiết lập kết nối thứ 2
- ✓ -dport (destination port): chỉ số port trên máy chủ được cho phép truy cập hoặc chặn
- ✓ -j <target>: Nhảy đến một target chain khi packet thỏa mãn luật hiện tại
  - ACCEPT: chấp nhập cho phép truy cập
  - DROP: không cho phép truy cập, không gửi phản hồi lại máy client
  - REJECT: không cho phép truy cập, và gửi phản hồi lại máy client.

3.2.2. Cho phép lưu lượng SNMP (Sử dụng UDP Port 161)

[root@localhost ~]# *iptables –A INPUT –p udp –m state –state NEW –m udp –dport 161 –J ACCEPT*

3.2.2. Cho phép lưu lượng HTTPs từ một địa chỉ IP (Sử dụng TCP Port 443)

[root@localhost ~]# *iptables –A INPUT –s 8.8.8.8 –p tcp –m state –state NEW –m tcp –dport 443 –j ACCEPT*

_ Trên đây là một số ví dụ cơ bản, bạn chỉ cần thay đổi các cổng, các giao thức và địa chỉ IP theo ý muốn của bạn cho phép các lưu lượng được phép truy cập.

_ Chúng ta có thể kiểm tra lại mọi thứ có đúng như chúng ta đã cấu hình hay không bằng cách sử dụng IPtables Status:

[root@localhost ~]# */etc/init.d/iptables status*

```
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
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 icmp-host-prohibited
6    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
7    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:161
8    ACCEPT     tcp  --  8.8.8.8              0.0.0.0/0           state NEW tcp dpt:443

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

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

[root@localhost ~]#
```

_ Nếu mọi thứ OK, chúng ta không thể quên việc lưu lại các luật đã tạo trên IPtables và khởi động lại những cấu hình đó của IPtables.

_ Bằng cách này, cấu hình đã được lưu vào file **/etc/sysconfig/iptables** và dịch vụ sẽ được khởi động:

[root@localhost ~]# */etc/init.d/iptables save*

[root@localhost ~]# */etc/init.d/iptables reload*

3.3. Xóa các luật trên IPtables

_ Trước khi chúng ta tiến hành xóa một luật nào đó trên IPtables, chúng ta cần kiểm tra lại các luật hiện tại đang chạy:

[root@localhost ~]# */etc/init.d/iptables status*

```
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
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 icmp-host-prohibited
6    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
7    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:161
8    ACCEPT     tcp  --  8.8.8.8              0.0.0.0/0           state NEW tcp dpt:443

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

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

[root@localhost ~]#
```

_ Nếu chúng ta muốn xóa luật: "**Cho phép lưu lượng SNMP (Sử dụng UDP Port 161)**" chúng ta sẽ sử dụng câu lệnh như sau:

[root@localhost ~]# *iptables –D INPUT 7* *# 7 là chỉ số dòng của luật trên IPtables*

_ Sau khi xóa luật ở dòng số 7, chúng ta có thể kiểm tra lại các luật hiện tại của IPtables

[root@localhost ~]# */etc/init.d/iptables status*

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

Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
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 icmp-host-prohibited
6    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
7    ACCEPT     tcp  --  8.8.8.8              0.0.0.0/0           state NEW tcp dpt:443

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

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

[root@localhost ~]#
```

_ Sau khi thực hiện việc xóa một luật nào đó từ IPtables, chúng ta không cần phải thực hiện việc khởi động lại dịch vụ của IPtables.

3.4. Cấu hình Luật cho IPtables (Theo cách tự lưu cấu hình)

_ Bây giờ bạn đã biết tự cấu hình Luật cho IPtables trên hệ thống của bạn. Có một điều nữa, tôi muốn nói thêm với các bạn.

_ Tôi nghĩ rằng, có một cách tốt hơn và dễ hơn để quản lý các luật của IPtables đó là quản lý thông qua file cấu hình **/etc/sysconfig/iptables**. Hình dưới đây, sẽ minh họa cấu hình mặc định của IPtables:

```
[root@localhost ~]# cat /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
# Generated by webmin
*nat
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
[root@localhost ~]#
```

_ Chúng ta có thể quản lý cấu hình của IPtables bằng cách sửa file **/etc/sysconfig/iptables** và khởi động lại dịch vụ IPtables.

_ Bằng cách sử dụng các trình soạn thảo thông dụng của Linux (ví dụ: vi), chúng ta có thể thêm hoặc xóa một luật nào đó của IPtables. Như bạn đã nhìn thấy có một luật mặc định của IPtables là cho phép truy cập SSH đến máy chủ Linux thông qua port 22, chúng ta có thể sử dụng luật đó copy và paste đồng thời thay đổi chỉ số port như mong muốn là chúng ta đã có một luật mới.

_ Với cách đó, chúng ta có thể thêm tất cả các luật từ bước 2 ở trên vào file cấu hình: **/etc/sysconfig/iptables:**

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A INPUT -s 8.8.8.8 -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
```

_ Sau khi thêm các luật vào file cấu hình của IPtables, chúng ta sẽ tiến hành khởi động lại dịch vụ IPtables:

[root@localhost ~]# */etc/init.d/iptables restart*

_ Đồng thời kiểm tra lại các luật hiện tại của IPtables:

root@localhost:~

```
[root@localhost ~]# /etc/init.d/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: mangle
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

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

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

Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
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:80
5    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           state NEW udp dpt:161
6    ACCEPT     tcp  --  8.8.8.8              0.0.0.0/0           state NEW tcp dpt:443
7    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
8    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
```

3.5 Xóa các luật của IPtables (Theo cách tự lưu cấu hình)

_ Để xóa một luật nào đó của IPtables, chúng ta có thể sử dụng công cụ soạn thảo (ví dụ: vi) của linux để tiến hành mở file **/etc/sysconfig/iptables** và đồng thời xóa luật nào mà chúng ta muốn xóa.

_ Sau khi xóa xong, chúng ta tiến hành lưu và thoát khỏi công cụ soạn thảo. Đồng thời khởi động lại dịch vụ IPtables.

CHƯƠNG IX: DNS

1) GIỚI THIỆU

DNS là viết tắt của cụm từ Domain Name System, mang ý nghĩa đầy đủ là **hệ thống phân giải tên miền**. Hiểu một cách ngắn gọn nhất, DNS cơ bản là một hệ thống chuyển đổi các tên miền website mà chúng ta đang sử dụng, ở dạng *www.abc.com* sang một địa chỉ IP dạng số tương ứng với **tên miền** đó và ngược lại.

2) MÔ HÌNH TRIỂN KHAI

- **Máy chủ DNS chính (Master):**
  - **HĐH:** CentOS 6.5 Server
  - **Hostname:** masterdns.abc.local
  - **Địa chỉ IP:** 192.168.1.100/24
- **Máy chủ DNS Backup (Slave):**
  - **HĐH:** CentOS 6.5 Server
  - **Hostname:** secondarydns.abc.local
  - **Địa chỉ IP:** 192.168.1.101/24
- **Máy Client:**
  - **HĐH:** Centos 6.5 Desktop
  - **Hostname:** Client.abc.local
  - **Địa chỉ IP:** 192.168.1.102/24

3) CÀI ĐẶT VÀ CẤU HÌNH DNS

3.1. Cài đặt máy chủ DNS chính (Master)

[root@masterdns ~]# *yum install bind* -y*

3.1.1. Cấu hình máy chủ DNS

_ Thêm những dòng bôi đỏ vào file **"/etc/named.conf"**

[root@masterdns ~]# **vi /etc/named.conf**

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
```

```
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
listen-on port 53 { 127.0.0.1; 192.168.1.100; }; ### Master DNS IP ###
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     { localhost; 192.168.1.0/24; }; ### IP Range ###
allow-transfer{ localhost; 192.168.1.101; };   ### Slave DNS IP ###
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
managed-keys-directory "/var/named/dynamic";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
type hint;
file "named.ca";
};
zone"abc.local" IN {
type master;
file "forward.abc";
allow-update { none; };
};
zone"1.168.192.in-addr.arpa" IN {
type master;
file "reverse.abc";
allow-update { none; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

3.1.2. Tạo các file Zone

_ Tiến hành tạo Forward Zone và Reverse Zone trong file **"/etc/named.conf"**

a. Tạo Forward Zone

_ Tạo file **forward.abc** trong thư mục **'/var/named'**

[root@masterdns ~]# **vi /var/named/forward.abc**

```
$TTL 86400
@   IN  SOA    masterdns.abc.local. root.abc.local. (
       2011071001  ;Serial
       3600       ;Refresh
       1800       ;Retry
       604800     ;Expire
       86400      ;Minimum TTL
)
@      IN  NS        masterdns.abc.local.
@      IN  NS        secondarydns.abc.local.
@      IN  A         192.168.1.100
@      IN  A         192.168.1.101
@      IN  A         192.168.1.102
masterdns      IN  A   192.168.1.100
secondarydns   IN  A   192.168.1.101
client         IN  A   192.168.1.102
```

b. Tạo Reverse Zone

_Tạo file **reverse.abc** trong thư mục **'/var/named'**

[root@masterdns ~]# **vi /var/named/reverse.abc**

```
$TTL 86400
@   IN  SOA    masterdns.abc.local. root.abc.local. (
       2011071001  ;Serial
       3600       ;Refresh
       1800       ;Retry
       604800     ;Expire
       86400      ;Minimum TTL
)
@      IN  NS        masterdns.abc.local.
@      IN  NS        secondarydns.abc.local.
@      IN  PTR       abc.local.
masterdns      IN  A   192.168.1.100
secondarydns   IN  A   192.168.1.101
client         IN  A   192.168.1.102
100    IN  PTR       masterdns.abc.local.
101    IN  PTR       secondarydns.abc.local.
102    IN  PTR       client.abc.local.
```

3.1.3. Khởi động dịch vụ DNS

[root@masterdns ~]# **service named start**

Starting named: [OK]

[root@masterdns ~]# **chkconfig named on**

3.1.4. Cấu hình IPtables để cho phép truy cập DNS Server từ mạng ngoài

_ Sửa file cấu hình **'/etc/sysconfig/iptables'**

[root@masterdns ~]# **vi /etc/sysconfig/iptables**

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p udp -m state --state NEW --dport 53 -j ACCEPT
-A INPUT -p tcp -m state --state NEW --dport 53 -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

3.1.5. Khởi động lại IPtables

[root@masterdns ~]# **service iptables restart**

```
iptables: Flushing firewall rules:                  [  OK  ]
iptables: Setting chains to policy ACCEPT: filter   [  OK  ]
iptables: Unloading modules:                        [  OK  ]
iptables: Applying firewall rules:                  [  OK  ]
```

3.1.6. Kiểm tra cấu hình DNS và các file Zone

```
[root@masterdns ~]# named-checkconf /etc/named.conf
[root@masterdns ~]# named-checkzone abc.local /var/named/forward.abc
zone abc.local/IN: loaded serial 2011071001
```

OK

[root@masterdns ~]# named-checkzone abc.local /var/named/reverse.abc

zone abc.local/IN: loaded serial 2011071001

OK

3.1.7. Kiểm tra máy chủ DNS

[root@masterdns ~]# **dig masterdns.abc.local**

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6_3.6 <<>> masterdns.abc.local

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49834

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:

;masterdns.abc.local.INA

;; ANSWER SECTION:

masterdns.abc.local. 86400INA192.168.1.100

;; AUTHORITY SECTION:

abc.local.86400INNSsecondarydns.abc.local.

abc.local.86400INNSmasterdns.abc.local.

;; ADDITIONAL SECTION:

secondarydns.abc.local. 86400 INA192.168.1.101

;; Query time: 6 msec

;; SERVER: 192.168.1.100#53(192.168.1.100)

;; WHEN: Thu Mar 7 13:07:56 2013

;; MSG SIZE rcvd: 114

[root@masterdns ~]# **nslookup abc.local**

Server:192.168.1.100

Address:192.168.1.100#53

Name:abc.local

Address: 192.168.1.102

Name:abc.local

Address: 192.168.1.100

Name:abc.local

Address: 192.168.1.101

_ Bây giờ, máy chủ DNS chính (Master) đã sẵn sàng để hoạt động.

3.2 Cài đặt máy chủ DNS backup (slave)

[root@secondarydns ~]# **yum install bind* -y**

3.2.1 Cấu hình máy chủ DNS backup

_ Mở file cấu hình **/etc/named.conf** và thêm các dòng bôi đỏ như bên dưới:

[root@secondarydns ~]# **vi /etc/named.conf**

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
listen-on port 53 { 127.0.0.1; 192.168.1.101; };
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     { localhost; 192.168.1.0/24; };
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
```

```
managed-keys-directory "/var/named/dynamic";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
type hint;
file "named.ca";
};
zone"abc.local" IN {
type slave;
file "slaves/abc.fwd";
masters { 192.168.1.100; };
};
zone"1.168.192.in-addr.arpa" IN {
type slave;
file "slaves/abc.rev";
masters { 192.168.1.100; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

3.2.2 Khởi động dịch vụ DNS

```
[root@secondarydns ~]# service named start
Generating /etc/rndc.key:                          [  OK  ]
Starting named:                                    [  OK  ]
[root@secondarydns ~]# chkconfig named on
```

_ Tạo Forward zone và Reverse zone trên máy chủ DNS backup trong file **/var/named/slaves,** để cho phép tự động đồng bộ cấu hình với máy chủ DNS chính.

[root@secondarydns ~]# **ls /var/named/slaves/**

abc.fwd abc.rev

[root@secondarydns ~]# **cat /var/named/slaves/abc.fwd**

$ORIGIN .

$TTL 86400; 1 day

abc.localIN SOAmasterdns.abc.local. root.abc.local. (

2011071001 ; serial

3600 ; refresh (1 hour)

1800 ; retry (30 minutes)

604800 ; expire (1 week)

86400 ; minimum (1 day)

)

NS masterdns.abc.local.

NS secondarydns.abc.local.

A192.168.1.100

A192.168.1.101

A192.168.1.102

$ORIGIN abc.local.

clientA192.168.1.102

masterdnsA192.168.1.100

secondarydnsA192.168.1.101

[root@secondarydns ~]# **cat /var/named/slaves/abc.rev**

$ORIGIN .

$TTL 86400; 1 day

1.168.192.in-addr.arpaIN SOAmasterdns.abc.local. root.abc.local. (

2011071001 ; serial

3600 ; refresh (1 hour)

1800 ; retry (30 minutes)

604800 ; expire (1 week)

86400 ; minimum (1 day)

)

NS masterdns.abc.local.

NS secondarydns.abc.local.

PTRabc.local.

$ORIGIN 1.168.192.in-addr.arpa.

100PTRmasterdns.abc.local.

101PTRsecondarydns.abc.local.

102PTRclient.abc.local.

clientA192.168.1.102

masterdnsA192.168.1.100

secondarydnsA192.168.1.101

3.2.3 Thêm các thông số chi tiết của máy chủ DNS vào tất cả hệ thống

[root@secondarydns ~]# vi /etc/resolv.conf

Generated by NetworkManager

search ostechnix.com

nameserver 192.168.1.100

nameserver 192.168.1.101

nameserver 8.8.8.8

3.2.4 Kiểm tra máy chủ DNS

[root@secondarydns ~]# dig masterdns.abc.local

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6_3.6 <<>> masterdns.abc.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21487
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; QUESTION SECTION:
;masterdns.abc.local.INA
;; ANSWER SECTION:
masterdns.abc.local. 86400INA192.168.1.100
;; AUTHORITY SECTION:
abc.local.86400INNSmasterdns.abc.local.
abc.local.86400INNSsecondarydns.abc.local.
;; ADDITIONAL SECTION:

secondarydns.abc.local. 86400 INA192.168.1.101
;; Query time: 15 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Thu Mar 7 13:27:57 2013
;; MSG SIZE rcvd: 114

[root@secondarydns ~]# **dig secondarydns.abc.local**
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6_3.6 <<>> secondarydns.abc.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20958
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; QUESTION SECTION:
;secondarydns.abc.local.INA
;; ANSWER SECTION:
secondarydns.abc.local. 86400 INA192.168.1.101
;; AUTHORITY SECTION:
abc.local.86400INNSmasterdns.abc.local.
abc.local.86400INNSsecondarydns.abc.local.
;; ADDITIONAL SECTION:
masterdns.abc.local. 86400INA192.168.1.100
;; Query time: 4 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Thu Mar 7 13:31:53 2013
;; MSG SIZE rcvd: 114

[root@secondarydns ~]# **nslookup abc.local**
Server:192.168.1.100
Address:192.168.1.100#53
Name:abc.local
Address: 192.168.1.101
Name:abc.local
Address: 192.168.1.102
Name:abc.local
Address: 192.168.1.100

3.3 Cấu hình Client

_ Tiến hành thêm chi tiết các thông số của máy chủ DNS vào file **/etc/resolv.conf** vào toàn bộ các thiết bị Client trên hệ thống

[root@client abc]# **vi /etc/resolv.conf**
Generated by NetworkManager
search abc.local
nameserver 192.168.1.100
nameserver 192.168.1.101

nameserver 8.8.8.8

_ Test máy chủ DNS

```
[root@client abc]# dig masterdns.abc.local
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6 <<>> masterdns.abc.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19496
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; QUESTION SECTION:
;masterdns.abc.local.INA
;; ANSWER SECTION:
masterdns.abc.local. 86400INA192.168.1.100
;; AUTHORITY SECTION:
abc.local.86400INNSmasterdns.abc.local.
abc.local.86400INNSsecondarydns.abc.local.
;; ADDITIONAL SECTION:
secondarydns.abc.local. 86400 INA192.168.1.101
;; Query time: 30 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Thu Mar  7 13:47:55 2013
;; MSG SIZE  rcvd: 114
```

```
[root@client abc]# dig secondarydns.abc.local
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6 <<>> secondarydns.abc.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14852
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; QUESTION SECTION:
;secondarydns.abc.local.INA
;; ANSWER SECTION:
secondarydns.abc.local. 86400 INA192.168.1.101
;; AUTHORITY SECTION:
abc.local.86400INNSsecondarydns.abc.local.
abc.local.86400INNSmasterdns.abc.local.
;; ADDITIONAL SECTION:
masterdns.abc.local. 86400INA192.168.1.100
;; Query time: 8 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Thu Mar  7 13:48:38 2013
;; MSG SIZE  rcvd: 114
```

```
[root@client abc]# dig client.abc.local
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.10.rc1.el6 <<>> client.abc.local
```

;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14604
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
;client.abc.local.INA
;; ANSWER SECTION:
client.abc.local.86400INA192.168.1.102
;; AUTHORITY SECTION:
abc.local.86400INNSmasterdns.abc.local.
abc.local.86400INNSsecondarydns.abc.local.
;; ADDITIONAL SECTION:
masterdns.abc.local. 86400INA192.168.1.100
secondarydns.abc.local. 86400 INA192.168.1.101
;; Query time: 5 msec
;; SERVER: 192.168.1.100#53(192.168.1.100)
;; WHEN: Thu Mar 7 13:49:11 2013
;; MSG SIZE rcvd: 137

[root@client abc]# **nslookup abc.local**
Server:192.168.1.100
Address:192.168.1.100#53
Name:abc.local
Address: 192.168.1.102
Name:abc.local
Address: 192.168.1.100
Name:abc.local
Address: 192.168.1.101

CHƯƠNG X: MAIL SERVER

1) GIỚI THIỆU

_ Cài đặt máy chủ Mail nội bộ sử dụng Postfix, Dovecot và Squirrelmail

_ **Postfix** là chương trình mã nguồn mở và miễn phí (free and open-source) dùng để gửi thư điện tử (Mail Transfer Agent – MTA) được tạo ra ban đầu tại IBM với mục tiêu là thay thế chương trình gửi mail phổ biến là Sendmail. Postfix được phát triển dựa trên mục tiêu là nhanh, dễ quản lý và bảo mật.

_ **Dovecot** cũng là phần mềm miễn phí mã nguồn mở được dùng để nhận email bằng IMAP và POP3. Dovecot nhanh, dễ dàng cài đặt, dễ quản lý, bảo mật cao và sử dụng rất ít bộ nhớ

_ **SquirrelMail** là một trong những ứng dụng email trên Web phổ biến nhất được viết bằng PHP. Nó được tích hợp sẵn hỗ trợ PHP thuần túy cho IMAP và SMTP, bên cạnh đó nó được thiết kết để hiển thị tất cả các trang trong HTML mà không cần đến JavaScript, để có khả năng tương thích tối đa trên các trình duyệt.

2) MÔ HÌNH TRIỂN KHAI

- ✓ **HĐH:** CentOS 6.5
- ✓ **Địa chỉ IP:** 192.168.1.101/24
- ✓ **Hostname:** server.abc.local

3) CÀI ĐẶT VÀ CẤU HÌNH MAIL SERVER

- ➢ **Bước 1:** Gỡ bỏ phần mềm Sendmail

_ Trước khi tiến hành cài đặt, chúng ta cần gỡ bỏ phần mềm Sendmail được cài mặc định trên các hệ thống Linux (nếu có)

 # yum remove sendmail

- ➢ **Bước 2: Cấu hình máy chủ DNS**

_ Cấu hình máy chủ DNS và thêm các bản ghi MX của máy chủ Mail vào trong file forward zone và reverse zone.

_ Để cài đặt máy chủ DNS, chúng ta có thể xem lại Chương IX – DNS.

_ Chúng ta cũng cần liên hệ với ISP để chỏ IP Public về domain của Email (Nếu có)

- ➢ **Bước 3: Sửa file Hosts**

_ Thêm dòng mới như bên dưới vào file **/etc/hosts**

 # vi /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

192.168.1.101 server.abc.local server

- **Bước 4: Tắt dịch vụ SELinux**

_ Tắt dịch vụ SELinux để hạn chế sự phức tạp trong quá trình cấu hình Postfix.

 # vi /etc/selinux/config

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
# enforcing - SELinux security policy is enforced.
# permissive - SELinux prints warnings instead of enforcing.
# disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
# targeted - Only targeted network daemons are protected.
# strict - Full SELinux protection.
SELINUXTYPE=targeted
```

_ Khởi động lại máy chủ.

- **Bước 5: Cài đặt EPEL Repo**

_ Chúng ta sẽ sử dụng Squirrelmail cho Webmail client. Squirrelmail sẽ không được tìm thấy trên Cen tOS Repo, vì vậy chúng ta cần tiến hành cài đặt EPEL Repo.

 # wget http://epel.mirror.net.in/epel/6/i386/epel-release-6-8.noarch.rpm

 # rpm -Uvh epel-release-6-8.noarch.rpm

 # yum repolist

- **Bước 6: Cấu hình Firewall mở port 80**

 # vi /etc/sysconfig/iptables

[...]

-A INPUT -m state --state NEW -m tcp -p tcp --**dport** 80 -j ACCEPT

[...]

3.1 Cài đặt Postfix

_ Tiến hành cài đặt gói Postfix trên máy chủ Mail:

 # yum install postfix –y

3.2 Cấu hình Postfix

_ Sửa file **/etc/postfix/main.cf,**

 # vi /etc/postfix/main.cf

_ Tìm kiếm và sửa những dòng sau:

Line no 75 - Uncomment and set your mail server FQDN

myhostname = server.abc.local

Line 83 - Uncomment and Set domain name

mydomain = abc.local

Line 99 - Uncomment

myorigin = $mydomain

Line 116 - Set ipv4

inet_interfaces = all

Line 119 - Change to all

inet_protocols = all

Line 164 - Comment

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

Line 165 - Uncomment ##\

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

Line 264 - Uncomment and add IP range

mynetworks = 192.168.1.0/24, 127.0.0.0/8

Line 419 - Uncomment

home_mailbox = Maildir/

_ Lưu và thoát khỏi file, đồng thời khởi động dịch vụ Postfix:

 # service postfix restart

 # chkconfig postfix on

3.3 Kiểm tra máy chủ Mail Postfix

_ Tạo một tài khoản kiểm tra là "SK"

 # useradd sk

 # passwd sk

_ Truy cập vào máy chủ thông qua Telnet và nhập vào những dòng lệnh như dưới đây:

```
# telnet localhost smtp
Trying ::1...
Connected to localhost.
Escape character is '^]'.
220 server.abc.local ESMTP Postfix
ehlo localhost     ## type this command ##
250-server.abc.local
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from:<sk>     ## Type this - mail sender address##
250 2.1.0 Ok
rcpt to:<sk>     ## Type this - mail receiver address ##
250 2.1.5 Ok
data     ## Type this to input email message ##
354 End data with <CR><LF>.<CR><LF>
welcome to abc mail server     ## Enter the boddy of the email ##.
    ## type dot (.) to complete message ##
250 2.0.0 Ok: queued as B822221522
quit     ## type this to quit from mail ##
221 2.0.0 Bye
Connection closed by foreign host.
```

_ Mở thư mục mail của tài khoản **"sk"** và kiểm tra mail mới

```
# ls /home/sk/Maildir/new/
1390215275.Vfd00Ie04f8M357080.server.abc.local
```

_ Một Email mới đã được nhận bởi tài khoản "sk". Để đọc nội dung email, sử dụng lệnh sau:

```
# cat /home/sk/Maildir/new/1390215275.Vfd00Ie04f8M357080.server.abc.local
Return-Path: <sk@abc.local>
X-Original-To: sk
Delivered-To: sk@abc.local
Received: from localhost (localhost [IPv6:::1])
   by server.abc.local (Postfix) with ESMTP id B822221522
   for <sk>; Mon, 20 Jan 2014 16:23:54 +0530 (IST)
Message-Id: <20140120105404.B822221522@server.abc.local>
Date: Mon, 20 Jan 2014 16:23:54 +0530 (IST)
From: sk@abc.local
To: undisclosed-recipients:;
welcome to abc mail server
```

3.4 Cài đặt Dovecot

```
# yum install dovecot
```

3.4.1 Cấu hình Dovecot

_ Sửa file **/etc/dovecot/dovecot.conf,**

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

_ Bỏ comment những dòng bên dưới:

```
## Line 20 - umcomment ##
protocols = imap pop3 lmtp
```

_ Sửa file **/etc/dovecot/conf.d/10-mail.conf**

```
# vi /etc/dovecot/conf.d/10-mail.conf
## Line 24 - uncomment ##
mail_location = maildir:~/Maildir
```

_ Sửa file /etc/dovecot/conf.d/10-auth.conf

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

line 9 - uncomment##

disable_plaintext_auth = yes

Line 97 - Add a letter "login"

auth_mechanisms = plain login

_ Sửa file /etc/dovecot/conf.d/10-master.conf

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

Line 83, 84 - Uncomment and add "postfix"

#mode = 0600

user = postfix

group = postfix

_ Khởi động dịch vụ Dovecot:

service dovecot start

chkconfig dovecot on

3.4.2 Kiểm tra Dovecot

_ Để kiểm tra Dovecot, thực hiện truy cập vào máy chủ Mail thông qua telnet như bên dưới:

telnet localhost pop3

Trying ::1...

Connected to localhost.

Escape character is '^]'.

+OK Dovecot ready.

user sk ## log in as user sk ##

+OK

pass centos ## input user password ##

+OK Logged in.

retr 1

+OK 439 octets

Return-Path: <sk@abc.local>

X-Original-To: sk

Delivered-To: sk@abc.local

Received: from localhost (localhost [IPv6:::1])

by server.abc.local (Postfix) with ESMTP id B822221522

for <sk>; Mon, 20 Jan 2014 16:23:54 +0530 (IST)

Message-Id: <20140120105404.B822221522@server.abc.local>

Date: Mon, 20 Jan 2014 16:23:54 +0530 (IST)

From: sk@abc.local

To: undisclosed-recipients:;

welcome to abc mail server

.

quit

+OK Logging out.

Connection closed by foreign host.

3.5 Cài đặt Squirrelmail

_ Bạn cần chắc chắn máy chủ Mail của bạn đã cài đặt và bật **EPEL Repo**. Bây giờ, tiến hành cài đặt Squirrelmail sử dụng lệnh sau:

 # yum install squirrelmail -y

_ Chuyển vào thư mục: **/usr/share/squirrelmail/config/** và chạy lệnh **conf.pl**

 # cd /usr/share/squirrelmail/config/

 # ./conf.pl

_ Trình hướng dẫn cấu hình sẽ được mở ra. Nhập chọn "**1**" để cấu hình các tham số chi tiết:

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 >> 1

_ Trình hướng dẫn phụ bên trong sẽ tiếp tục được mở. Chọn **"1"** để sửa thông tin:

SquirrelMail Configuration : Read: config.php (1.4.0)

Organization Preferences

1. Organization Name : SquirrelMail
2. Organization Logo : ../images/sm_logo.png
3. Org. Logo Width/Height : (308/111)
4. Organization Title : SquirrelMail $version
5. Signout Page :
6. Top Frame : _top
7. Provider link : http://squirrelmail.org/
8. Provider name : SquirrelMail

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

Command >> 1

_ Nhập tên của tổ chức và nhấn chọn Enter:

We have tried to make the name SquirrelMail as transparent as
possible. If you set up an organization name, most places where
SquirrelMail would take **credit** will be credited to your organization.

If your Organization Name includes a '$', please precede it with a \.
Other '$' will be considered the beginning of a variable that
must be defined before the $org_name is printed.
$version, for example, is included by default, and will print the
string representing the current SquirrelMail version.

[SquirrelMail]: Abc

_ Bằng cách này tương tự, chúng ta có thể cấu hình thông số chi tiết cho tổ chức như: title, logo, Provider Name trong trình hướng dẫn. Nhận chọn **"s"** để lưu những thay đổi và nhấn chọn **"R"** để quay trở lại trình hướng dẫn chính ban đầu:

SquirrelMail Configuration : Read: config.php (1.4.0)

Organization Preferences

1. Organization Name : Abc
2. Organization Logo : ../images/sm_logo.png
3. Org. Logo Width/Height : (308/111)
4. Organization Title : SquirrelMail $version
5. Signout Page :
6. Top Frame : _top
7. Provider link : http://squirrelmail.org/
8. Provider name : Abc Mail

R Return to Main Menu

C Turn color off

S Save data

Q Quit

Command >> s

_ Nhấn chọn **"2"** để cài đặt các thông số cho máy chủ Mail như tên miền và mail agent ….

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 >> 2

_ Chọn **"1"** và nhập vào tên miền của bạn và nhấn Enter:

SquirrelMail Configuration : Read: config.php (1.4.0)

Server Settings

General

---

1. Domain : localhost

2. Invert Time : false

3. Sendmail or SMTP : Sendmail

A. Update IMAP Settings : localhost:143 (uw)

B. Change Sendmail Config : /usr/sbin/sendmail

R Return to Main Menu

C Turn color off

S Save data

Q Quit

Command >> 1

The domain name is the suffix at the end of all email addresses. If

for example, your email address is jdoe@example.com, then your domain

would be example.com.

[localhost]: abc.local

_ Chọn **"3"** và thay đổi từ Sendmail thành Postfix:

SquirrelMail Configuration : Read: config.php (1.4.0)

Server Settings

General

---

1. Domain : abc.local
2. Invert Time : false
3. Sendmail or SMTP : Sendmail

A. Update IMAP Settings : localhost:143 (uw)

B. Change Sendmail Config : /usr/sbin/sendmail

R Return to Main Menu

C Turn color off

S Save data

Q Quit

Command >> 3

_ Chọn **"2"** để chuyển từ Sendmail sang Postfix

You now need to choose the method that you will use for sending messages in SquirrelMail. You can either connect to an SMTP server or use sendmail directly.

1. **Sendmail**

2. SMTP

Your choice [1/2] [1]: 2

_ Bây giờ, Nhấn chọn **"S"** để lưu cấu hình và chọn **"Q"** để thoát khỏi chế độ cấu hình của Squirrelmail

_ Tạo một Squirrelmail vhost trong file cấu hình Apache

vi **/etc/httpd/conf/**httpd.conf

```
Alias /webmail /usr/share/squirrelmail
<Directory /usr/share/squirrelmail>
   Options Indexes FollowSymLinks
   RewriteEngine On
   AllowOverride All
   DirectoryIndex index.php
   Order allow,deny
   Allow from all
</Directory>
```

_ Khởi động dịch vụ Apache:

 # service httpd restart

_ Tạo user để tiến hành sử dụng Email:

 # useradd abc1

 # useradd abc2

 # passwd 123456

 # passwd 123456

_ Truy cập Webmail: http://192.168.1.101/webmail