LAB 5

SAMBA, DNS và Firewall

> Họ tên và MSSV: **Nguyễn Văn Nhẫn - B1809272**
>
> Nhóm học phần: **Nhóm 02**

1. Cài đặt CentOS

(KHÔNG cần hình minh họa):

1.1. Thực hiện cài đặt CentOS 6 (hoặc CentOS 7/8) vào máy tính cá nhân (hoặc máy ảo).

1.2. Cấu hình mạng cho máy ảo giao tiếp được với máy vật lý và kết nối được vào Internet. **1.3.** Cài đặt dịch vụ Web server trên máy ảo. Tạo một trang web đơn giản index.html lưu vào thư mục /var/www/html/myweb **1.4.** Nếu sử dụng CentOS 6 thì cần thay đổi file cấu hình của yum theo hướng dẫn ở đây.

2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các nền tảng khác nhau như Windows và Linux bằng cách sử dụng giao thức SMB/CIFS. Trong bài thực hành sinh viên sẽ cài đặt và cấu hình dịch vụ Samba trên máy chủ CentOS và sử dụng máy Windows để truy cập tới dịch vụ.

2.1. Cài đặt dịch vụ Samba: `yum install samba`

```
[root@localhost B1809272]# yum install samba
Last metadata expiration check: 0:15:26 ago on Sun Apr 18 04:24:07 2021.
Dependencies resolved.
================================================================================
 Package                 Architecture     Version                 Repository        Size
================================================================================
Installing:
 samba                   x86_64           4.12.3-12.el8.3         baseos           840 k
Installing dependencies:
 samba-common-tools      x86_64           4.12.3-12.el8.3         baseos           484 k
 samba-libs              x86_64           4.12.3-12.el8.3         baseos           188 k

Transaction Summary
================================================================================
Install  3 Packages

Total download size: 1.5 M
Installed size: 4.0 M
Is this ok [y/N]: y
Downloading Packages:
(1/3): samba-libs-4.12.3-12.el8.3.x86_64.rpm                  791 kB/s | 188 kB     00:00
(2/3): samba-common-tools-4.12.3-12.el8.3.x86_64.rpm          1.9 MB/s | 484 kB     00:00
(3/3): samba-4.12.3-12.el8.3.x86_64.rpm                       2.9 MB/s | 840 kB     00:00
--------------------------------------------------------------------------------
Total                                                         1.5 MB/s | 1.5 MB     00:00
Running transaction check
Transaction check succeeded.
```

2.2. Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

```
adduser tuanthai
passwd tuanthai
groupadd lecturers
usermod -aG lecturers tuanthai
```

```
[root@localhost B1809272]# adduser nhandev && passwd nhandev
Changing password for user nhandev.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost B1809272]# groupadd lecturers && usermod -aG lecturers nhandev
[root@localhost B1809272]# groups nhandev
nhandev : nhandev lecturers
[root@localhost B1809272]#
```

2.3. Tạo thư mục cần chia sẻ và phân quyền:

```
mkdir /data
chgrp lecturers /data
chmod -R 775 /data
```

```
[root@localhost B1809272]# mkdir /data
[root@localhost B1809272]# chgrp lecturers /data
[root@localhost B1809272]# chmod -R 775 /data
[root@localhost B1809272]# ls -l / | grep data
drwxrwxr-x.   2 root lecturers    6 Apr 18 05:23 data
[root@localhost B1809272]#
```

2.4. Cấu hình dịch vụ Samba:

```
cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
nano /etc/samba/smb.conf
....
[data]
    comment = Shared folder for lecturers
    path = /data
        browsable = yes
    writable = yes
    read only = no
    valid users = @lecturers
```

```
[root@localhost B1809272]# cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[root@localhost B1809272]#
```

```
 GNU nano 2.9.8                                  /etc/samba/smb.conf

        printable = Yes
        create mask = 0600
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @printadmin root
        force group = @printadmin
        create mask = 0664
        directory mask = 0775
[data]
        comment = Shared folder for lecturers
        path = /data
        browsable = yes
        writable = yes
        read only = no
        valid users = @lecturers
```

2.5. Thêm người dùng cho dịch vụ Samba: `smbpasswd -a tuanthai`

```
[root@localhost B1809272]# smbpasswd -a nhandev
New SMB password:
Retype new SMB password:
Added user nhandev.
[root@localhost B1809272]#
```

2.6. Cấu hình SELINUX cho phép Samba

```
setsebool -P samba_export_all_rw on
setsebool -P samba_enable_home_dirs on
```

```
[root@localhost B1809272]# setsebool -P samba_export_all_rw on
[root@localhost B1809272]# setsebool -P samba_enable_home_dirs on
[root@localhost B1809272]#
```

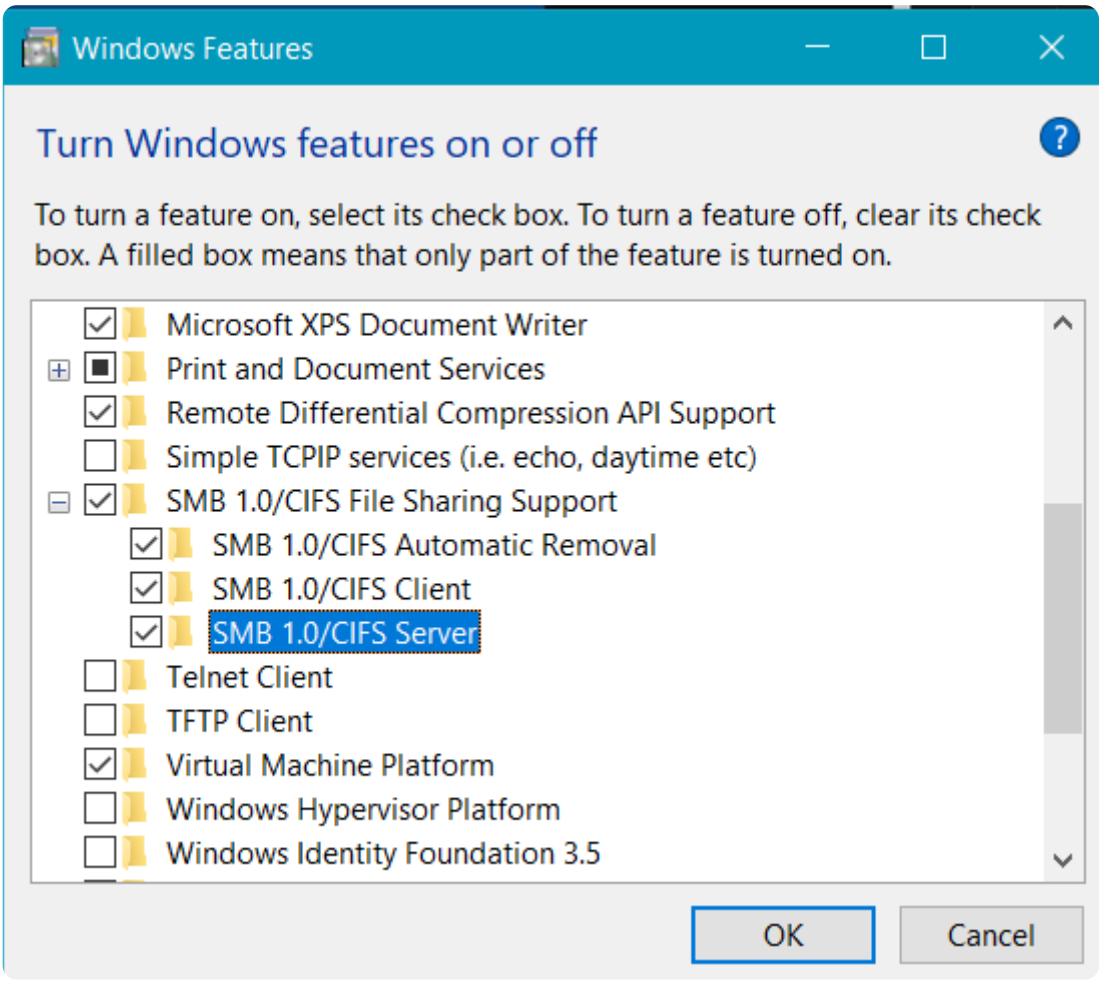
2.7. Tắt tường lửa: `service iptables stop`

```
[root@localhost B1809272]# service iptables stop
Redirecting to /bin/systemctl stop iptables.service
[root@localhost B1809272]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
   Active: inactive (dead) since Sun 2021-04-18 05:42:18 EDT; 3s ago
```

2.8. Khởi động dịch vụ Samba: `service smb start`

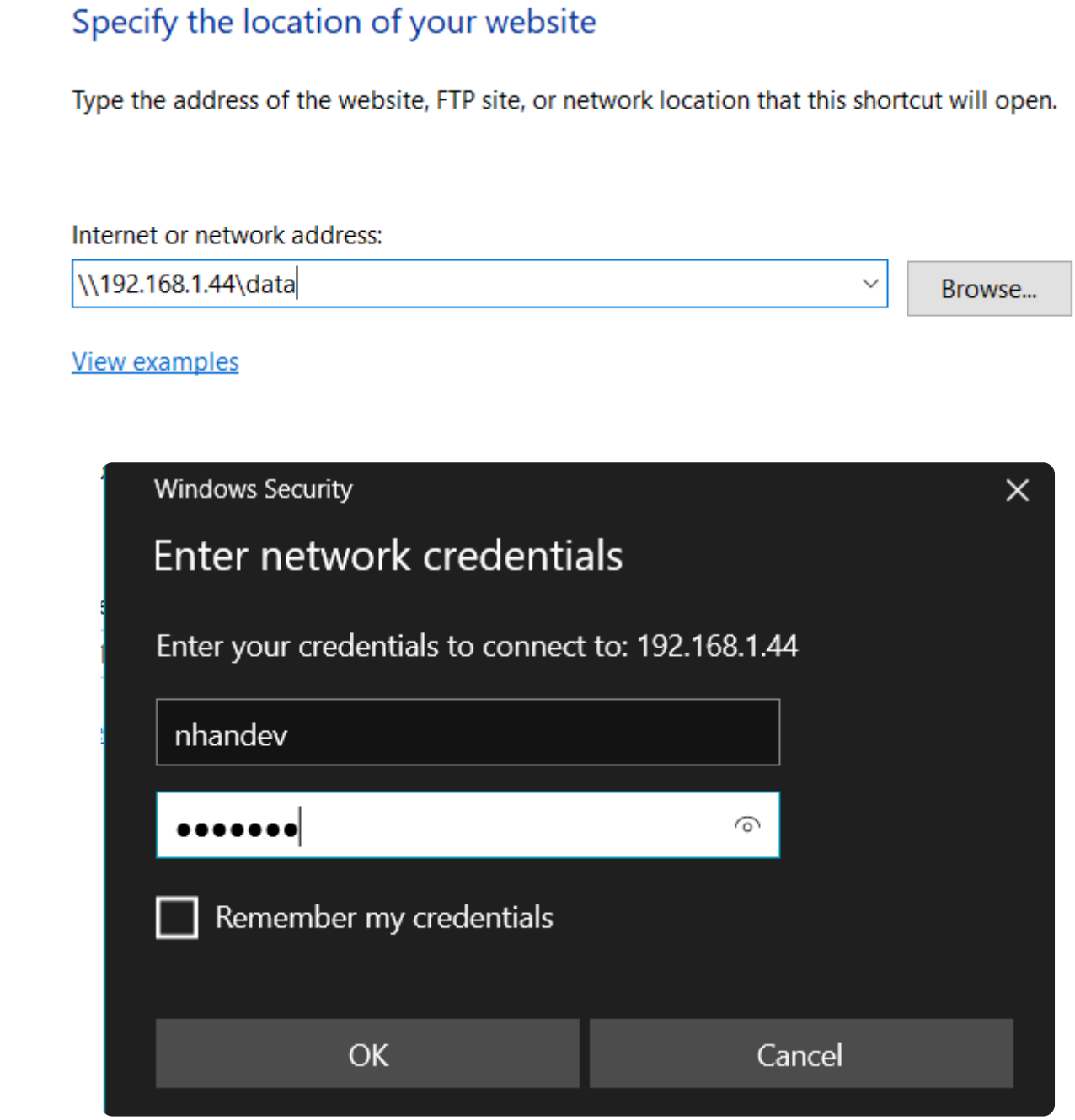
```
[root@localhost B1809272]# service smb start
Redirecting to /bin/systemctl start smb.service
[root@localhost B1809272]#
```

2.9. Trên máy Windows, bật tính năng hỗ trợ SMB1: mở Control Panel -> Programs -> Turn Windows features on or off -> SMB 1.0/CIFS File Sharing Support -> chọn SMB 1.0/CIFS Client



Nếu thực hành trong phòng máy của Khoa CNTT & TT có thể phải khởi động lại máy Windows. Trong trường hợp này sinh viên có thể qua bước 2.10

2.10. Trên File Explorer, chọn tính năng Add a network location để nối kết tới Samba server sử dụng địa chỉ `\\<IP máy CentOS>\data`



Trên máy CentOS tạo tập tin abc.txt

```
[root@localhost B1809272]# cat > /data/abc.txt
nguyen van nhan b1809272
^Z
[1]+  Stopped                 cat > /data/abc.txt
[root@localhost B1809272]#
```

Trên máy Window

3. Cài đặt và cấu hình dịch vụ DNS

DNS (Domain Name System) là giải pháp dùng tên miền thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng. Truy cập đến website của Khoa CNTT-ĐH Cần thơ bằng địa chỉ nào dễ nhớ hơn ? http://203.162.36.146 hay http://www.cit.ctu.edu.vn Trong bài thực hành này sinh viên cần cài đặt phần mềm BIND trên CentOS để phân giải tên miền "**qtht.com.vn**"

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

3.1. Cài đặt BIND và các công cụ cần thiết: `yum install bind bind-utils`

```
[root@localhost B1809272]#  yum install bind bind-utils
Last metadata expiration check: 1:49:39 ago on Sun Apr 18 04:24:07 2021.
Package bind-utils-32:9.11.20-5.el8_3.1.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package          Architecture       Version                    Repository     Size
================================================================================
Installing:
 bind             x86_64             32:9.11.20-5.el8_3.1       appstream     2.1 M

Transaction Summary
================================================================================
Install  1 Package

Total download size: 2.1 M
Installed size: 4.5 M
Is this ok [y/N]: y
Downloading Packages:
bind-9.11.20-5.el8_3.1.x86_64.rpm                 2.7 MB/s | 2.1 MB     00:00
--------------------------------------------------------------------------------
Total                                             1.3 MB/s | 2.1 MB     00:01
```

3.2. Cấu hình DNS server: `nano /etc/named.conf` (tham khảo file mẫu)

```
...
options {
    listen-on port 53 { 127.0.0.1; any;};
    ...
allow-query     { localhost; any; };
    recursion yes;
    ..
};

logging {
       ..
        };
};

zone "." IN {
    ...
};

zone "qtht.com.vn" IN {
    type master;
    file "forward.qtht";
    allow-update { none; };
```

```
};

zone "33.30.172.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
    allow-update { none; };
};
...
```

```
options {
        listen-on port 53 { 127.0.0.1;any };
        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";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost;any };
```

```
zone "qtht.com.vn" IN {
        type master;
        file "forward.qtht";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "reverse.qtht";
        allow-update { none; };
};
```

3.3. Tạo tập tin cấu hình phân giải xuôi:

```
cp /var/named/named.localhost /var/named/forward.qtht
chgrp named /var/named/forward.qtht
nano /var/named/forward.qtht
```

```
[root@localhost B1809272]# cat /var/named/named.localhost
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
[root@localhost B1809272]# cp /var/named/named.localhost /var/named/forward.qtht
[root@localhost B1809272]#
```

```
[root@localhost B1809272]# chgrp named /var/named/forward.qtht
[root@localhost B1809272]# ls /var/named
data  dynamic  forward.qtht  named.ca  named.empty  named.localhost  named.loopback  slaves
[root@localhost B1809272]# ls -l /var/named
total 20
drwxrwx---. 2 named named    6 Mar  1 10:20 data
drwxrwx---. 2 named named    6 Mar  1 10:20 dynamic
-rw-r-----. 1 root  named  152 Apr 18 06:26 forward.qtht
-rw-r-----. 1 root  named 2253 Mar  1 10:21 named.ca
-rw-r-----. 1 root  named  152 Mar  1 10:21 named.empty
-rw-r-----. 1 root  named  152 Mar  1 10:21 named.localhost
-rw-r-----. 1 root  named  168 Mar  1 10:21 named.loopback
drwxrwx---. 2 named named    6 Mar  1 10:20 slaves
```

```
 GNU nano 2.9.8                  /var/named/forward.qtht                  Modified

$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H      ; minimum
)
@       IN      NS      dns.qtht.com.vn.
dns     IN      A       192.168.1.44
www     IN      A       192.168.1.44
htql    IN      A       8.8.8.8
```

3.4. Tạo tập tin cấu hình phân giải ngược:

```
cp /var/named/forward.qtht /var/named/reverse.qtht
chgrp named /var/named/reverse.qtht
```

```
[root@localhost B1809272]# cp /var/named/forward.qtht /var/named/reverse.qtht
[root@localhost B1809272]# chgrp named /var/named/reverse.qtht
[root@localhost B1809272]# ls -l  /var/named
total 24
drwxrwx---. 2 named named   23 Apr 18 06:42 data
drwxrwx---. 2 named named   60 Apr 18 06:54 dynamic
-rw-r-----. 1 root  named  208 Apr 18 06:54 forward.qtht
-rw-r-----. 1 root  named 2253 Mar  1 10:21 named.ca
-rw-r-----. 1 root  named  152 Mar  1 10:21 named.empty
-rw-r-----. 1 root  named  152 Mar  1 10:21 named.localhost
-rw-r-----. 1 root  named  168 Mar  1 10:21 named.loopback
-rw-r-----. 1 root  named  208 Apr 18 07:00 reverse.qtht
drwxrwx---. 2 named named    6 Mar  1 10:20 slaves
[root@localhost B1809272]#
```

```
nano /var/named/reverse.qtht
```

```
$TTL 1D
@    IN  SOA @ qtht.com.vn. (
                                0    ;Serial
                                1D   ;Refresh
                                1H   ;Retry
                                1W   ;Expire
                                3H   ;Minimum TTL
)
@    IN  NS   dns.qtht.com.vn.
dns  IN  A    172.30.33.245
245  IN       PTR www.qtht.com.vn.
```

```
 GNU nano 2.9.8                /var/named/reverse.qtht                Modified

$TTL 1D
@       IN SOA  @ qtht.com.vn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H      ; minimum
)

@       IN      NS      dns.qtht.com.vn.
dns     IN      A       1.168.192
44      IN      PTR     www.qtht.com.vn.
```

3.5. Tắt tường lửa: `service iptables stop`

```
[root@localhost B1809272]# service iptables stop
Redirecting to /bin/systemctl stop iptables.service
[root@localhost B1809272]#
```

3.6. Khởi động dịch vụ DNS: `service named start`

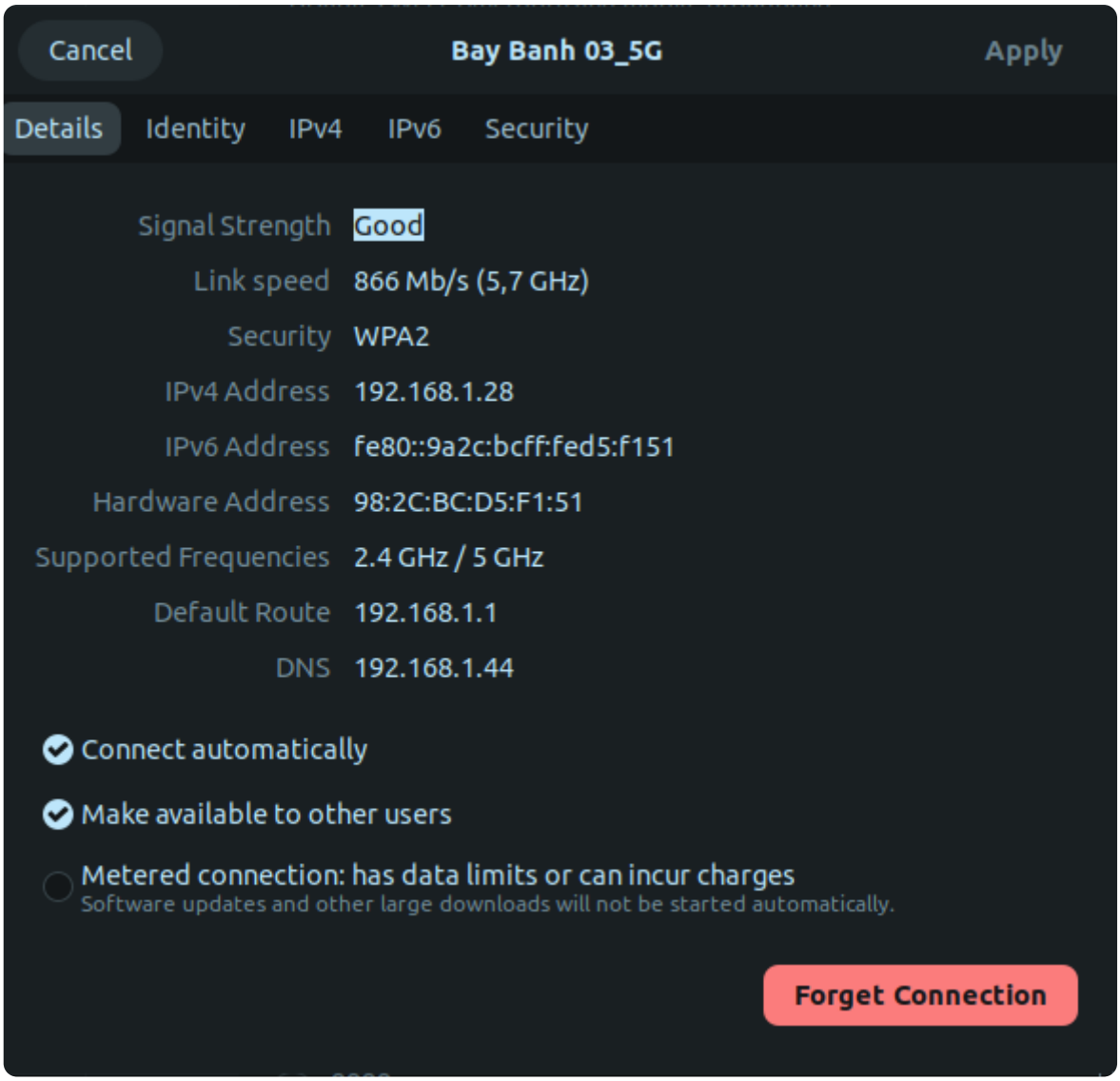
```
[root@localhost B1809272]# service named start
Redirecting to /bin/systemctl start named.service
[root@localhost B1809272]#
```

3.7. Kiểm tra kết quả: `nslookup www.qtht.com.vn <địa chỉ IP máy ảo>`

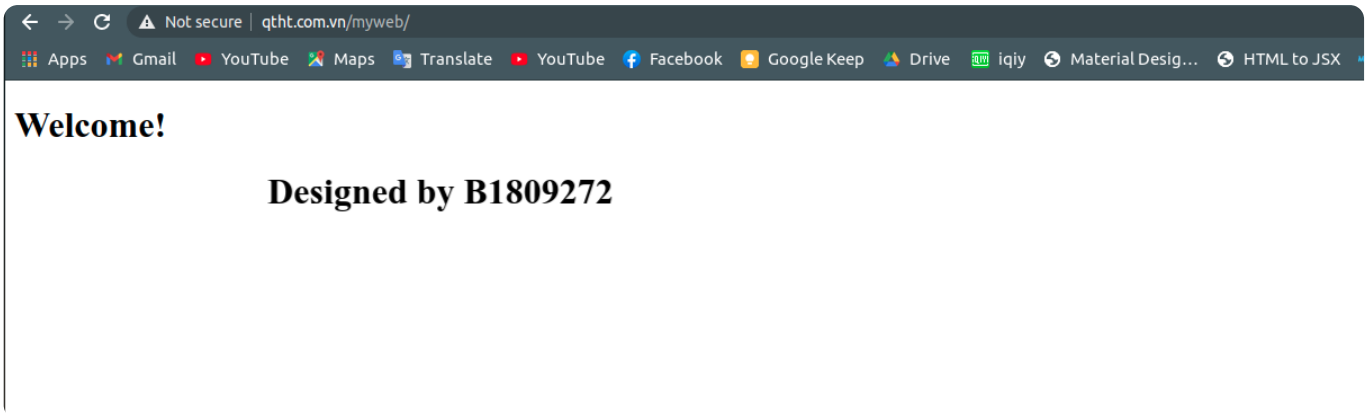
```
[root@localhost B1809272]# nslookup www.qtht.com.vn 192.168.1.44
Server:         192.168.1.44
Address:        192.168.1.44#53

Name:   www.qtht.com.vn
Address: 192.168.1.44

[root@localhost B1809272]# nslookup htql.qtht.com.vn 192.168.1.44
Server:         192.168.1.44
Address:        192.168.1.44#53

Name:   htql.qtht.com.vn
Address: 8.8.8.8

[root@localhost B1809272]#
```

```
[root@localhost B1809272]# nslookup 192.168.1.44 192.168.1.44
44.1.168.192.in-addr.arpa       name = www.qtht.com.vn.

[root@localhost B1809272]#
```

3.8. Trên máy vật lý, cấu hình DNS server là IP của máy ảo CentOS. Sau đó, mở trình duyệt web và truy cập vào địa chỉ http://www.qtht.com.vn/myweb


Cancel
Bay Banh 03_5G
Apply
Details
Identity
IPv4
IPv6
Security
Signal Strength
Good
Link speed
866 Mb/s (5,7 GHz)
Security
WPA2
IPv4 Address
192.168.1.28
IPv6 Address
fe80::9a2c:bcff:fed5:f151
Hardware Address
98:2C:BC:D5:F1:51
Supported Frequencies
2.4 GHz / 5 GHz
Default Route
192.168.1.1
DNS
192.168.1.44
Connect automatically
Make available to other users
Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.
Forget Connection


nvnhan@nvnhan-dev: ~
nvnhan@nvnhan-dev:~$ nslookup 192.168.1.44
44.1.168.192.in-addr.arpa name = www.qtht.com.vn.
Authoritative answers can be found from:
nvnhan@nvnhan-dev:~$ nslookup www.qtht.com.vn
Server: 127.0.0.53
Address: 127.0.0.53#53
Non-authoritative answer:
Name: www.qtht.com.vn
Address: 192.168.1.44



4.Cấu hình tường lửa iptables

iptables là một bộ công cụ được tích hợp trên hệ điều hành Linux để thực hiện chức năng tường lửa theo cơ chế lọc gói tin (packet filtering). iptables theo dõi lưu lượng mạng đến và đi ở một máy tính và lọc nó dựa trên dựa trên các luật (rules) do người dùng định nghĩa trước.

Tìm hiểu và thực hiện các yêu cầu sau (kèm hình minh họa cho từng bước):

4.1. Thực thi tường lửa iptables: `service iptables start`

```
[root@localhost b1809272]# service iptables start
Redirecting to /bin/systemctl start iptables.service
[root@localhost b1809272]# service iptables status
Redirecting to /bin/systemctl status iptables.service
● iptables.service - IPv4 firewall with iptables
   Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor pr>
   Active: active (exited) since Sat 2021-05-01 02:46:51 EDT; 5s ago
  Process: 115506 ExecStop=/usr/libexec/iptables/iptables.init stop (code=exite>
  Process: 115610 ExecStart=/usr/libexec/iptables/iptables.init start (code=exi>
 Main PID: 115610 (code=exited, status=0/SUCCESS)

May 01 02:46:51 localhost.localdomain systemd[1]: Starting IPv4 firewall with i>
May 01 02:46:51 localhost.localdomain iptables.init[115610]: iptables: Applying>
May 01 02:46:51 localhost.localdomain systemd[1]: Started IPv4 firewall with ip>
lines 1-10/10 (END)
```

4.2. Hiển thị các rules hiện có trên iptables `iptables -v -L --line-numbers`

```
[root@localhost b1809272]# iptables -v -L --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       96  7428 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
2        0     0 ACCEPT     icmp --  any    any     anywhere             anywhere
3        0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
4        0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             state NEW tcp dpt:ssh
5      920 59875 REJECT     all  --  any    any     anywhere             anywhere             reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1        0     0 REJECT     all  --  any    any     anywhere             anywhere             reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT 247 packets, 25541 bytes)
num   pkts bytes target     prot opt in     out     source               destination
[root@localhost b1809272]#
```

4.2. Tạo rules để cho phép các máy khác truy cập tới dịch vụ Web trên server

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

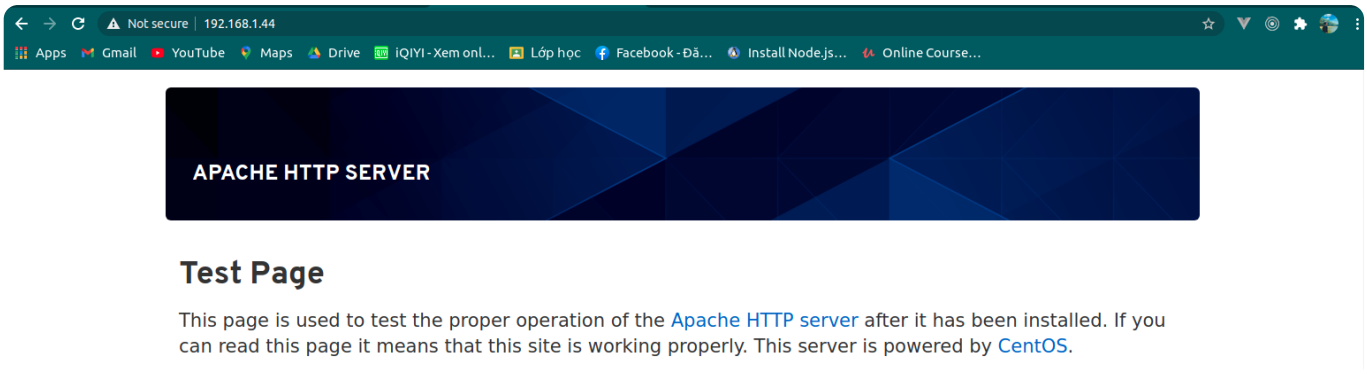
```
[root@localhost b1809272]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited
6    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1809272]#
```

```
iptables -D INPUT 6
```

```
[root@localhost b1809272]# iptables -D INPUT 6
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1809272]#
```

```
iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT
```

```
[root@localhost b1809272]# iptables -I INPUT 5 -p tcp --dport 80 -j ACCEPT
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  anywhere             anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
6    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1809272]#
```



4.4. Tạo rules để cho máy vật lý có thể ping tới server, các máy khác KHÔNG ping được.

```
iptables -D INPUT 2
```

```
[root@localhost b1809272]# iptables -D INPUT 2
[root@localhost b1809272]#
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     all  --  anywhere             anywhere
3    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
4    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
5    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1809272]#
```

```
nvnhan@nvnhan-dev:~$ ping 192.168.1.44
PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
From 192.168.1.44 icmp_seq=1 Destination Host Prohibited
From 192.168.1.44 icmp_seq=2 Destination Host Prohibited
From 192.168.1.44 icmp_seq=3 Destination Host Prohibited
From 192.168.1.44 icmp_seq=4 Destination Host Prohibited
^Z
[1]+  Stopped                 ping 192.168.1.44
nvnhan@nvnhan-dev:~$
```

```
iptables -I INPUT 2 -p icmp -s 192.168.1.28 -j ACCEPT
```

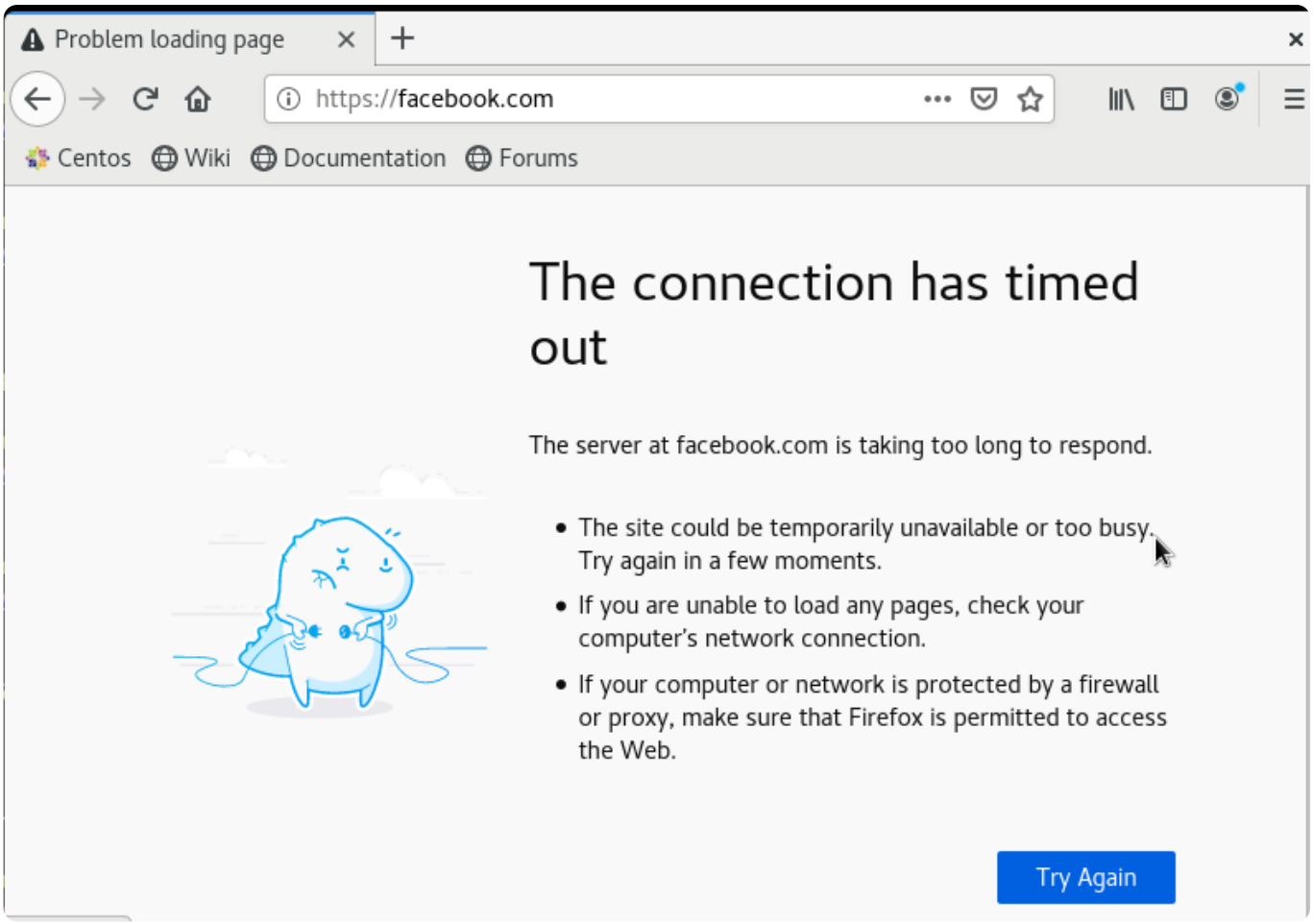
```
[root@localhost b1809272]# iptables -I INPUT 2 -p icmp -s 192.168.1.28 -j ACCEPT
[root@localhost b1809272]#
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.28         anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
6    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@localhost b1809272]#
```

```
nvnhan@nvnhan-dev:~$ ping 192.168.1.44
PING 192.168.1.44 (192.168.1.44) 56(84) bytes of data.
64 bytes from 192.168.1.44: icmp_seq=1 ttl=64 time=0.750 ms
64 bytes from 192.168.1.44: icmp_seq=2 ttl=64 time=0.348 ms
64 bytes from 192.168.1.44: icmp_seq=3 ttl=64 time=0.420 ms
64 bytes from 192.168.1.44: icmp_seq=4 ttl=64 time=0.449 ms
^Z
[1]+  Stopped                 ping 192.168.1.44
nvnhan@nvnhan-dev:~$
```

4.5. Tạo rules để KHÔNG cho người dùng trên máy CentOS truy cập tới địa chỉ facebook.com

```
iptables -A OUTPUT -p tcp -m string --string facebook --algo kmp -j REJECT
```

```
[root@localhost b1809272]# iptables -A OUTPUT -p tcp -m string --string facebook --algo kmp -j REJECT
[root@localhost b1809272]#
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.28         anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
6    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING match  "facebook" ALGO name
 kmp TO 65535 reject-with icmp-port-unreachable
[root@localhost b1809272]#
```



4.6. Lưu và phục hồi các luật của iptables

```
cp /etc/sysconfig/iptables /etc/sysconfig/iptables.orig
iptables-save > /etc/sysconfig/iptables
iptables-restore < /etc/sysconfig/iptables
```

```
[root@localhost b1809272]# cp /etc/sysconfig/iptables /etc/sysconfig/iptables.orig
[root@localhost b1809272]# iptables-save > /etc/sysconfig/iptables
[root@localhost b1809272]#
```

```
[root@localhost b1809272]# service iptables restart
Redirecting to /bin/systemctl restart iptables.service
[root@localhost b1809272]# iptables -L --line-number
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  anywhere             anywhere             state RELATED,ESTABLISHED
2    ACCEPT     icmp --  192.168.1.28         anywhere
3    ACCEPT     all  --  anywhere             anywhere
4    ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
5    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
6    REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

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

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     tcp  --  anywhere             anywhere             STRING match  "facebook" ALGO name
 kmp TO 65535 reject-with icmp-port-unreachable
[root@localhost b1809272]#
```