



LAB 5

DOCKER, SAMBA, DNS và Firewall

Họ tên và MSSV: Huỳnh Nhật Duy_B2110072

Nhóm học phần: CT17902

- Các sinh viên bị phát hiện sao chép bài của nhau sẽ nhận 0đ cho tất cả bài thực hành của môn này.
- Bài nộp phải ở dạng PDF, hình minh họa phải rõ ràng chi tiết. Hình minh họa chỉ cần chụp ở nội dung thực hiện, không chụp toàn màn hình.
- Video hướng dẫn ở cuối bài.

1. Triển khai dịch vụ WEB sử dụng Docker

- 1.1. Thực hiện cài đặt CentOS 9 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. (Câu 2 - Lab04)
- 1.3. Tạo thư mục ~/myweb, sau đó tạo một trang web đơn giản index.html lưu vào thư mục ~/myweb. (Câu 6 - Lab04)

Tắt tường lửa:

```
$sudo systemctl stop firewalld
```

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

- 1.4. Cài đặt Docker lên máy ảo CentOS 9
 - Gỡ bỏ PodMan (do sẽ đụng độ với Docker)

```
$sudo dnf -y remove podman runc
```

```
b2110072@server1:~  
[b2110072@server1 ~]$ sudo dnf -y remove podman runc  
Dependencies resolved.  
=====
```

Package	Arch	Version	Repository	Size
Removing:				
podman	x86_64	2:4.8.1-1.el9	@appstream	52 M
runc	x86_64	1.1.11-1.el9	@appstream	9.8 M

```
Removed:
cockpit-podman-82-1.el9.noarch          common-2:2.1.10-1.el9.x86_64
podman-2:4.8.1-1.el9.x86_64             runc-4:1.1.11-1.el9.x86_64
shadow-utils-subid-2:4.9-8.el9.x86_64

Complete!
[b2110072@server1 ~]$
```

- Cài đặt công cụ yum-utils

```
$sudo dnf install -y yum-utils
```

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo dnf install -y yum-utils
Last metadata expiration check: 1:13:34 ago on Wed 10 Apr 2024 06:34:10 PM +07.
Dependencies resolved.
=====
Package                                Arch      Version              Repository           Size
=====
Installing:
```

```
Upgraded:
dnf-plugins-core-4.3.0-13.el9.noarch
python3-dnf-plugins-core-4.3.0-13.el9.noarch
Installed:
yum-utils-4.3.0-13.el9.noarch

Complete!
[b2110072@server1 ~]$
```

- Thêm địa repo của Docker vào công cụ yum

```
$sudo yum-config-manager \
```

```
--add-repo \
```

```
https://download.docker.com/linux/centos/docker-ce.repo
```

#Viết liên tục lệnh trên hoặc xuống hàng bằng enter.

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo yum-config-manager \
--add-repo \
https://download.docker.com/linux/centos/docker-ce.repo
Adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
[b2110072@server1 ~]$
```

- Cài đặt Docker

```
$sudo dnf install docker-ce -y
```

```
b2110072@server1:~ — sudo dnf install docker-ce -y
[b2110072@server1 ~]$ sudo dnf install docker-ce -y
Docker CE Stable - x86_64                        88 kB/s | 41 kB      00:00
Last metadata expiration check: 0:00:01 ago on Wed 10 Apr 2024 07:53:20 PM +07.
Dependencies resolved.
=====
Package                                Arch      Version      Repository      Size
=====
```

```
Installed:
containerd.io-1.6.28-3.2.el9.x86_64
docker-buildx-plugin-0.13.1-1.el9.x86_64
docker-ce-3:26.0.0-1.el9.x86_64
docker-ce-cli-1:26.0.0-1.el9.x86_64
docker-ce-rootless-extras-26.0.0-1.el9.x86_64
docker-compose-plugin-2.25.0-1.el9.x86_64

Complete!
[b2110072@server1 ~]$
```

- Thêm người dùng hiện tại vào nhóm docker để sử dụng các lệnh của Docker mà không cần quyền sudo

```
$sudo usermod -aG docker $USER
```

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo usermod -aG docker $USER
[b2110072@server1 ~]$
```

- Login lại vào shell để việc thêm người dùng vào nhóm có tác dụng

```
$su - $USER
```

```
b2110072@server1:~ — -bash
[b2110072@server1 ~]$ su - $USER
Password:
[b2110072@server1 ~]$
```

- Chạy dịch vụ Docker

```
$sudo systemctl start docker
```

```
$sudo systemctl enable docker
```

```
b2110072@server1:~ — sudo systemctl status docker

[b2110072@server1 ~]$ sudo systemctl start docker
[b2110072@server1 ~]$ sudo systemctl enable docker
Created symlink /etc/systemd/system/multi-user.target.wants/docker.service → /usr/lib/systemd/system/docker.service.
[b2110072@server1 ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: d>
   Active: active (running) since Wed 2024-04-10 19:57:00 +07; 39s ago
 TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
    Main PID: 41057 (dockerd)
```

- Tạo 1 tài khoản trên DockerHub (<https://hub.docker.com/>), sau đó đăng nhập sử dụng lệnh sau:

```
$docker login -u <docker-username>
```

```
b2110072@server1:~ — -bash

[b2110072@server1 ~]$ docker login -u duynhut366
Password:
WARNING! Your password will be stored unencrypted in /home/b2110072/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
[b2110072@server1 ~]$
```

- Kiểm tra docker bằng cách tải image hello-world và tạo container tương ứng. Nếu xuất hiện thông điệp chào mừng từ Docker là cài đặt thành công.

```
$docker run hello-world
```

```
b2110072@server1:~ — -bash

[b2110072@server1 ~]$ docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:03b30c6a3c320ff172b52bd68eddfde6ded08ce47e650fe52de861c5e9df46d
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/
```

- 1.5. Triển khai dịch vụ web server lên máy ảo CentOS 9 sử dụng một Docker container
- Tìm kiếm image với từ khóa httpd, kết quả sẽ thấy 1 image tên httpd ở dòng đầu tiên.

\$docker search httpd

```
b2110072@server1:~ — -bash

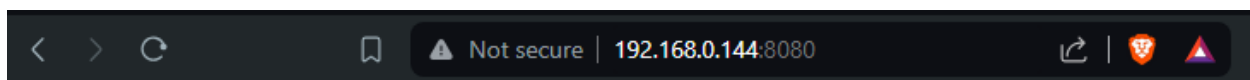
[b2110072@server1 ~]$ docker search httpd
NAME                                DESCRIPTION
STARS    OFFICIAL
httpd     The Apache HTTP Server Project
4692      [OK]
clearlinux/httpd    httpd HyperText Transfer Protocol (HTTP) ser...
5
paketobuildpacks/httpd
0
vulhub/httpd
0
jitesoft/httpd      Apache httpd on Alpine linux.
0
openquantumsafe/httpd
12    Demo of post-quantum cryptography in Apache ...
```

- Tạo container từ image httpd

\$docker run -d -it -p 8080:80 --name webserver httpd

- d: chạy container ở chế độ background
- it: tạo shell để tương tác với container
- name webserver: đặt tên container là webserver
- p 8080:80 gắn cổng 8080 của máy CentOS vào cổng 80 của container.

```
b2110072@server1:~ — -bash
[b2110072@server1 ~]$ docker run -d -it -p 8080:80 --name webserver httpd
Unable to find image 'httpd:latest' locally
latest: Pulling from library/httpd
8a1e25ce7c4f: Pull complete
419e34c9abe5: Pull complete
4f4fb700ef54: Pull complete
ab0f05d928ee: Pull complete
b8600f2091fe: Pull complete
3cdcad84146a: Pull complete
Digest: sha256:bb17569997412ca504a8058694a71f4f4219614de8d51689c25924c69f17c62a
Status: Downloaded newer image for httpd:latest
43f7271f9f7695da3ebae83b193c19863140045ef58495523a20ab1b3ed7e10f
[b2110072@server1 ~]$
```



It works!

- Sao chép thư mục ~/myweb vào thư mục gốc của dịch vụ của web trên Docker container.
\$docker cp myweb/ webserver:/usr/local/apache2/htdocs/

```
b2110072@server1:~ — -bash
[b2110072@server1 ~]$ docker cp myweb/ webserver:/usr/local/apache2/htdocs/
Successfully copied 2.56kB to webserver:/usr/local/apache2/htdocs/
[b2110072@server1 ~]$
```

- Trên máy vật lý, mở trình duyệt web và truy cập vào địa chỉ `http://<Địa chỉ IP máy ảo CentOS>:8080/myweb` để kiểm chứng trang web vừa tạo.



2. Cài đặt và cấu hình dịch vụ SAMBA

Samba là dịch vụ chia sẻ file giữa các hệ điều hành 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.

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

- Cài đặt dịch vụ Samba:

```
$sudo dnf install -y samba
```

A screenshot of a terminal window titled 'b2110072@server1:~ — sudo dnf install -y samba'. The terminal shows the command 'sudo dnf install -y samba' being executed. It prompts for a password, shows the metadata expiration check, and lists the packages to be installed. The output shows that several packages were upgraded and several were installed.

```
[b2110072@server1 ~]$ sudo dnf install -y samba
[sudo] password for b2110072:
Last metadata expiration check: 0:39:21 ago on Wed 10 Apr 2024 07:53:20 PM +07.
Dependencies resolved.
=====
Package                               Arch           Version           Repository        Size
-----
Upgraded:
  libsmclient-4.19.4-104.el9.x86_64    libwbclient-4.19.4-104.el9.x86_64
  samba-client-libs-4.19.4-104.el9.x86_64  samba-common-4.19.4-104.el9.noarch
  samba-common-libs-4.19.4-104.el9.x86_64
Installed:
  libnetapi-4.19.4-104.el9.x86_64
  samba-4.19.4-104.el9.x86_64
  samba-common-tools-4.19.4-104.el9.x86_64
  samba-dcerpc-4.19.4-104.el9.x86_64
  samba-ldb-ldap-modules-4.19.4-104.el9.x86_64
  samba-libs-4.19.4-104.el9.x86_64

Complete!
[b2110072@server1 ~]$
```

- Tạo người dùng và nhóm người dùng chia sẻ dữ liệu:

```
$sudo adduser tuanthai
```

```
$sudo passwd tuanthai
```

```
$sudo groupadd lecturers
```

```
$sudo usermod -a -G lecturers tuanthai
```

```
b2110072@server1:~ — -bash
[b2110072@server1 ~]$ sudo adduser duynhut
[b2110072@server1 ~]$ sudo passwd duynhut
Changing password for user duynhut.
New password:
BAD PASSWORD: The password is a palindrome
Retype new password:
passwd: all authentication tokens updated successfully.
[b2110072@server1 ~]$ sudo groupadd lecturers
[b2110072@server1 ~]$ sudo usermod -a -G lecturers duynhut
[b2110072@server1 ~]$
```

- Tạo thư mục cần chia sẻ và phân quyền:

```
$sudo mkdir /data
$sudo chown :lecturers /data
$sudo chmod -R 775 /data
```

```
b2110072@server1:/data
[b2110072@server1 ~]$ cd /data
[b2110072@server1 data]$ sudo chown :lecturers /data
[b2110072@server1 data]$ sudo chmod -R 775 /data
[b2110072@server1 data]$
```

- Cấu hình dịch vụ Samba:

```
$sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
$sudo nano /etc/samba/smb.conf
#Thêm đoạn cấu hình bên dưới vào cuối tập tin
[data]
    comment = Shared folder for lecturers
    path = /data
    browsable = yes
    writable = yes
    read only = no
    valid users = @lecturers
```

```
b2110072@server1:/data
[b2110072@server1 data]$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.orig
[b2110072@server1 data]$ sudo nano /etc/samba/smb.conf
[b2110072@server1 data]$
```



```
b2110072@server1:/data
GNU nano 5.6.1 /etc/samba/smb.conf Modified
comment = All Printers
path = /var/tmp
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
```

- Thêm người dùng cho dịch vụ Samba:
\$sudo smbpasswd -a tuanthai
#Đặt mật khẩu Samba cho người dùng

```
b2110072@server1:/data
[b2110072@server1 data]$ sudo smbpasswd -a duynhut
New SMB password:
Retype new SMB password:
Added user duynhut.
[b2110072@server1 data]$
```

- Cấu hình SELINUX cho phép Samba
\$sudo setsebool -P samba_export_all_rw on
\$sudo setsebool -P samba_enable_home_dirs on

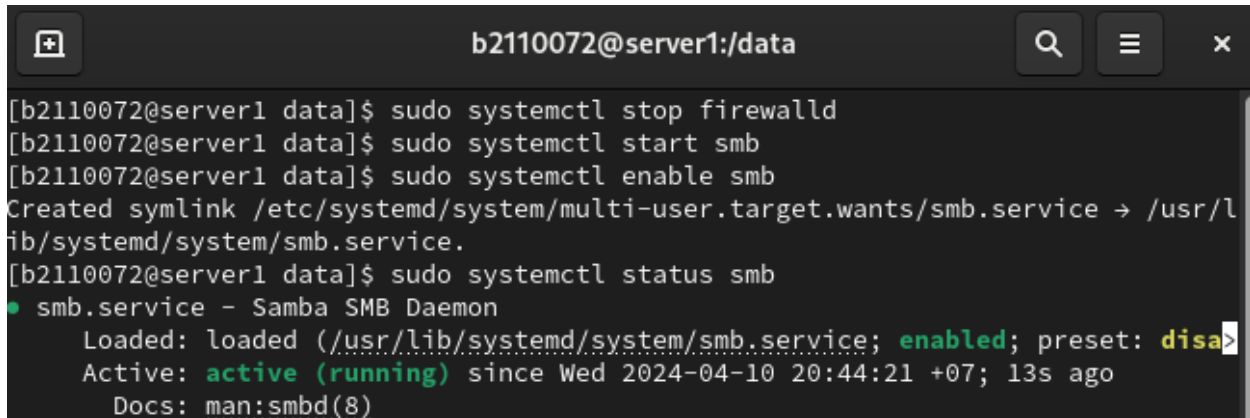
```
b2110072@server1:/data
[b2110072@server1 data]$ sudo setsebool -P samba_export_all_rw on
[b2110072@server1 data]$ sudo setsebool -P samba_enable_home_dirs on
[b2110072@server1 data]$
```

- Tắt tường lửa:
\$sudo systemctl stop firewalld

- Khởi động cho phép Samba tự động thực thi khi khởi động hệ điều hành:

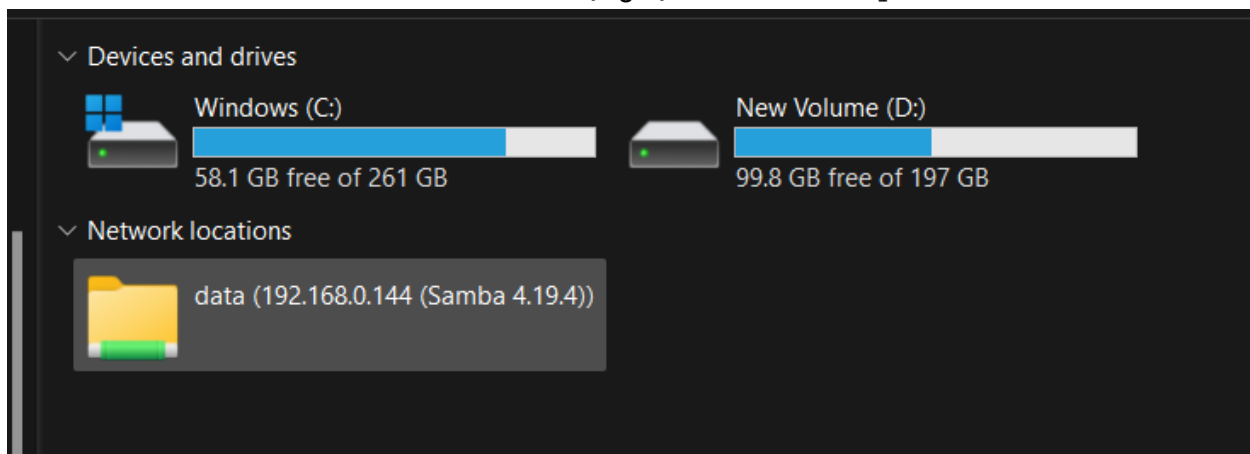
```
$sudo systemctl start smb
```

```
$sudo systemctl enable smb
```



```
b2110072@server1:/data
[b2110072@server1 data]$ sudo systemctl stop firewallld
[b2110072@server1 data]$ sudo systemctl start smb
[b2110072@server1 data]$ sudo systemctl enable smb
Created symlink /etc/systemd/system/multi-user.target.wants/smb.service → /usr/lib/systemd/system/smb.service.
[b2110072@server1 data]$ sudo systemctl status smb
● smb.service - Samba SMB Daemon
   Loaded: loaded (/usr/lib/systemd/system/smb.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-04-10 20:44:21 +07; 13s ago
     Docs: man:smbd(8)
```

- Trên File Explorer của máy Windows, chọn tính năng “Add a network location” để nối kết tới Samba server sử dụng địa chỉ \\<IP máy CentOS>\data



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 Trường CNTT-TT- Trường ĐH Cần Thơ bằng địa chỉ nào dễ nhớ hơn ?

<http://123.30.143.202> 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:

```
$sudo dnf install bind bind-utils -y
```

```
b2110072@server1:/data
[b2110072@server1 data]$ sudo dnf install bind bind-utils -y
Last metadata expiration check: 1:08:08 ago on Wed 10 Apr 2024 07:53:20 PM +07.
Package bind-utils-32:9.16.23-14.el9.x86_64 is already installed.
Dependencies resolved.
=====
Package                Arch      Version                Repository      Size
=====
Installing:
```

```
Upgraded:
  bind-libs-32:9.16.23-15.el9.x86_64    bind-license-32:9.16.23-15.el9.noarch
  bind-utils-32:9.16.23-15.el9.x86_64
Installed:
  bind-32:9.16.23-15.el9.x86_64
  bind-dnssec-doc-32:9.16.23-15.el9.noarch
  bind-dnssec-utils-32:9.16.23-15.el9.x86_64
  python3-bind-32:9.16.23-15.el9.noarch
  python3-ply-3.11-14.el9.noarch

Complete!
[b2110072@server1 data]$
```

3.2. Cấu hình DNS server:

\$sudo nano /etc/named.conf

```
b2110072@server1:/data
[b2110072@server1 data]$ nmcli -f ipv4.dns con show enp0s3
ipv4.dns:                                192.168.0.1
[b2110072@server1 data]$
```

#(tham khảo file mẫu)

```
...
options {
    listen-on port 53 { 127.0.0.1; any; };
    ...
    allow-query      { localhost; any; };
    recursion yes;
    forwarders {192.168.55.1; };
    ..
};

logging {
    ..
```

```

        };

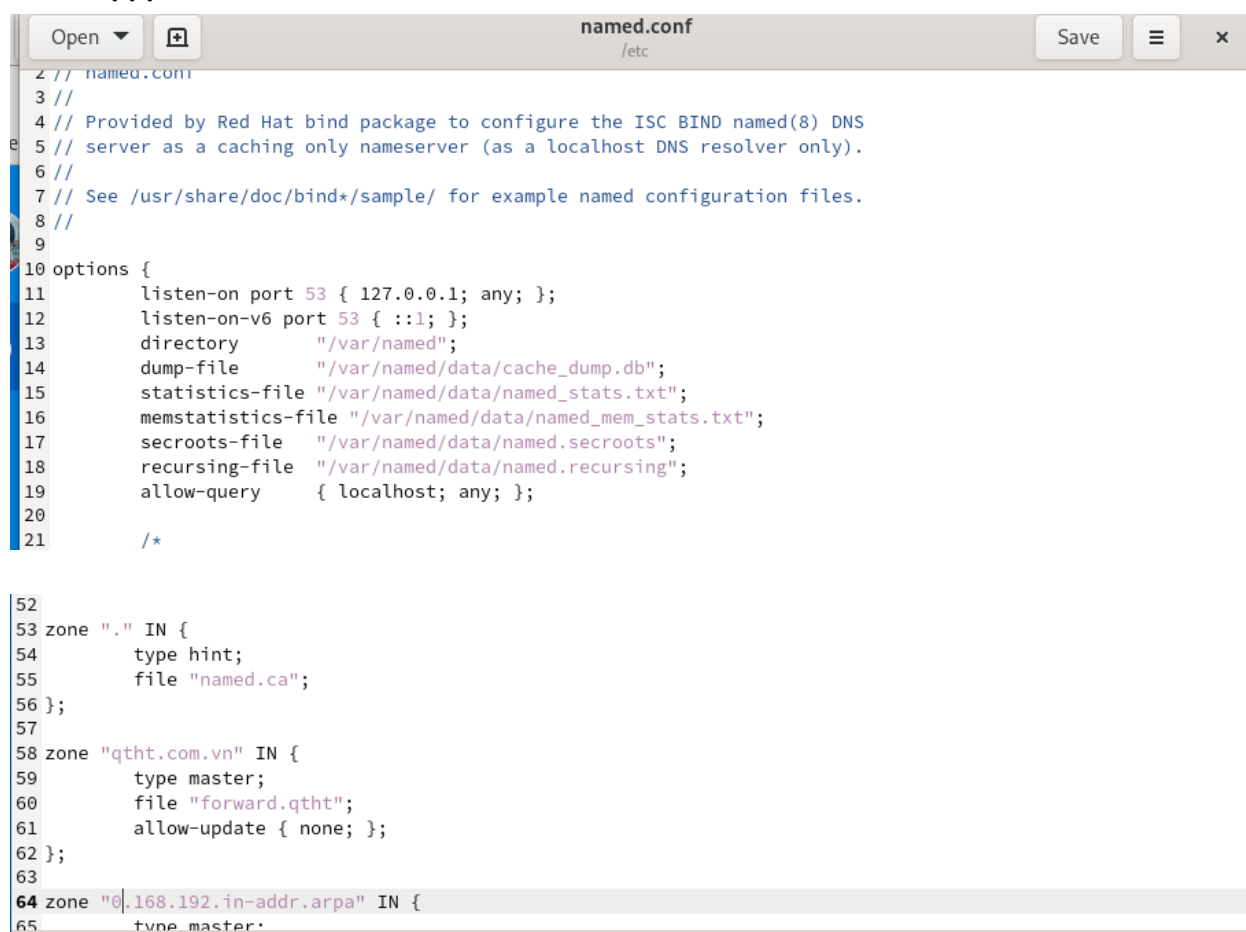
};

zone "." IN {
    ...
};

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

zone "55.168.192.in-addr.arpa" IN {
    type master;
    file "reverse.qtht";
    allow-update { none; };
};
...

```



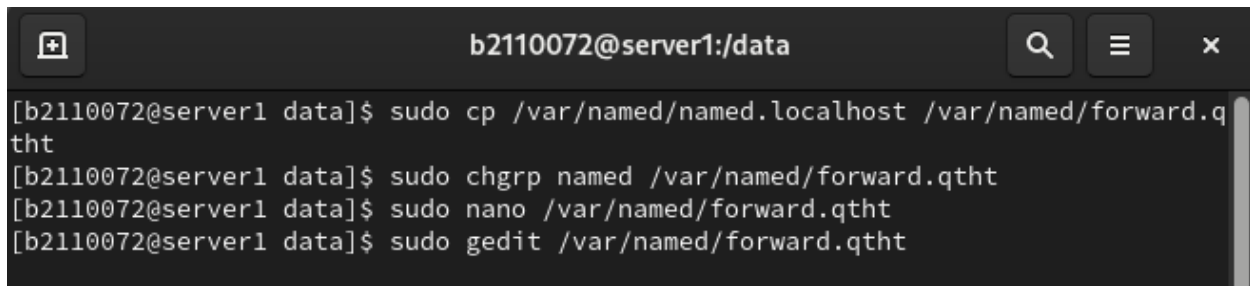
```

2 // named.conf
3 //
4 // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5 // server as a caching only nameserver (as a localhost DNS resolver only).
6 //
7 // See /usr/share/doc/bind*/sample/ for example named configuration files.
8 //
9
10 options {
11     listen-on port 53 { 127.0.0.1; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory "/var/named";
14     dump-file "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file "/var/named/data/named.secrets";
18     recursing-file "/var/named/data/named.recursing";
19     allow-query { localhost; any; };
20
21     /*
52
53 zone "." IN {
54     type hint;
55     file "named.ca";
56 };
57
58 zone "qtht.com.vn" IN {
59     type master;
60     file "forward.qtht";
61     allow-update { none; };
62 };
63
64 zone "0.168.192.in-addr.arpa" IN {
65     type master;

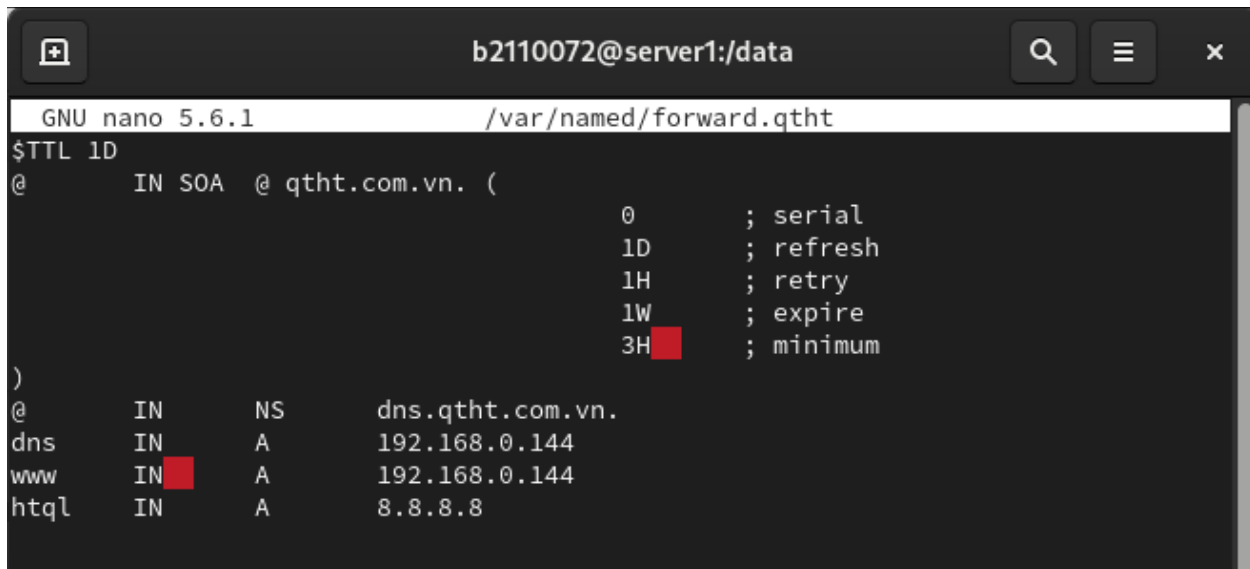
```

3.3. Tạo tập tin cấu hình phân giải xuôi:

```
$sudo cp /var/named/named.localhost /var/named/forward.qtht
$sudo chgrp named /var/named/forward.qtht
$sudo nano /var/named/forward.qtht
#(tham khảo file mẫu)
$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    192.168.55.250
www    IN      A    192.168.55.250
htql   IN      A    8.8.8.8
```



```
b2110072@server1:/data
[b2110072@server1 data]$ sudo cp /var/named/named.localhost /var/named/forward.qtht
[b2110072@server1 data]$ sudo chgrp named /var/named/forward.qtht
[b2110072@server1 data]$ sudo nano /var/named/forward.qtht
[b2110072@server1 data]$ sudo gedit /var/named/forward.qtht
```



```
GNU nano 5.6.1 /var/named/forward.qtht
$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    192.168.0.144
www    IN      A    192.168.0.144
htql   IN      A    8.8.8.8
```

3.4. Tạo tập tin cấu hình phân giải ngược:

```
$sudo cp /var/named/forward.qtht /var/named/reverse.qtht
$sudo chgrp named /var/named/reverse.qtht
$sudo 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    192.168.55.250
250    IN      PTR  www.qtht.com.vn.
```

```
b2110072@server1:/data
[b2110072@server1 data]$ sudo cp /var/named/forward.qtht /var/named/reverse.qtht
[sudo] password for b2110072:
[b2110072@server1 data]$ sudo chgrp named /var/named/reverse.qtht
[b2110072@server1 data]$ sudo nano /var/named/reverse.qtht
[b2110072@server1 data]$
```

```
GNU nano 5.6.1 /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    192.168.0.144
1      IN      PTR  www.qtht.com.vn.
```

3.5. Kiểm tra và sử dụng dịch vụ DNS

- Tắt tường lửa:
\$sudo systemctl stop firewalld
- Khởi động dịch vụ DNS:
\$sudo systemctl start named

```
b2110072@server1:/data
[b2110072@server1 data]$ sudo systemctl stop firewalld
[b2110072@server1 data]$ sudo systemctl start named
[b2110072@server1 data]$ sudo systemctl status named
• named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; preset: disabled)
   Active: active (running) since Wed 2024-04-10 21:24:24 +07; 19s ago
     Process: 47788 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" ==>
     Process: 47791 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS >
    Main PID: 47792 (named)
      Tasks: 8 (limit: 17255)
     Memory: 33.7M
        CPU: 62ms
```

- Kiểm tra kết quả:

```
nslookup www.qtht.com.vn <địa chỉ IP máy ảo>
nslookup htql.qtht.com.vn <địa chỉ IP máy ảo>
nslookup www.ctu.edu.vn <địa chỉ IP máy ảo>
```

```
b2110072@server1:/data
[b2110072@server1 data]$ nslookup www.qtht.com.vn 192.168.0.144
Server:          192.168.0.144
Address:         192.168.0.144#53

Name:   www.qtht.com.vn
Address: 192.168.0.1

[b2110072@server1 data]$ nslookup htql.qtht.com.vn 192.168.0.144
Server:          192.168.0.144
Address:         192.168.0.144#53

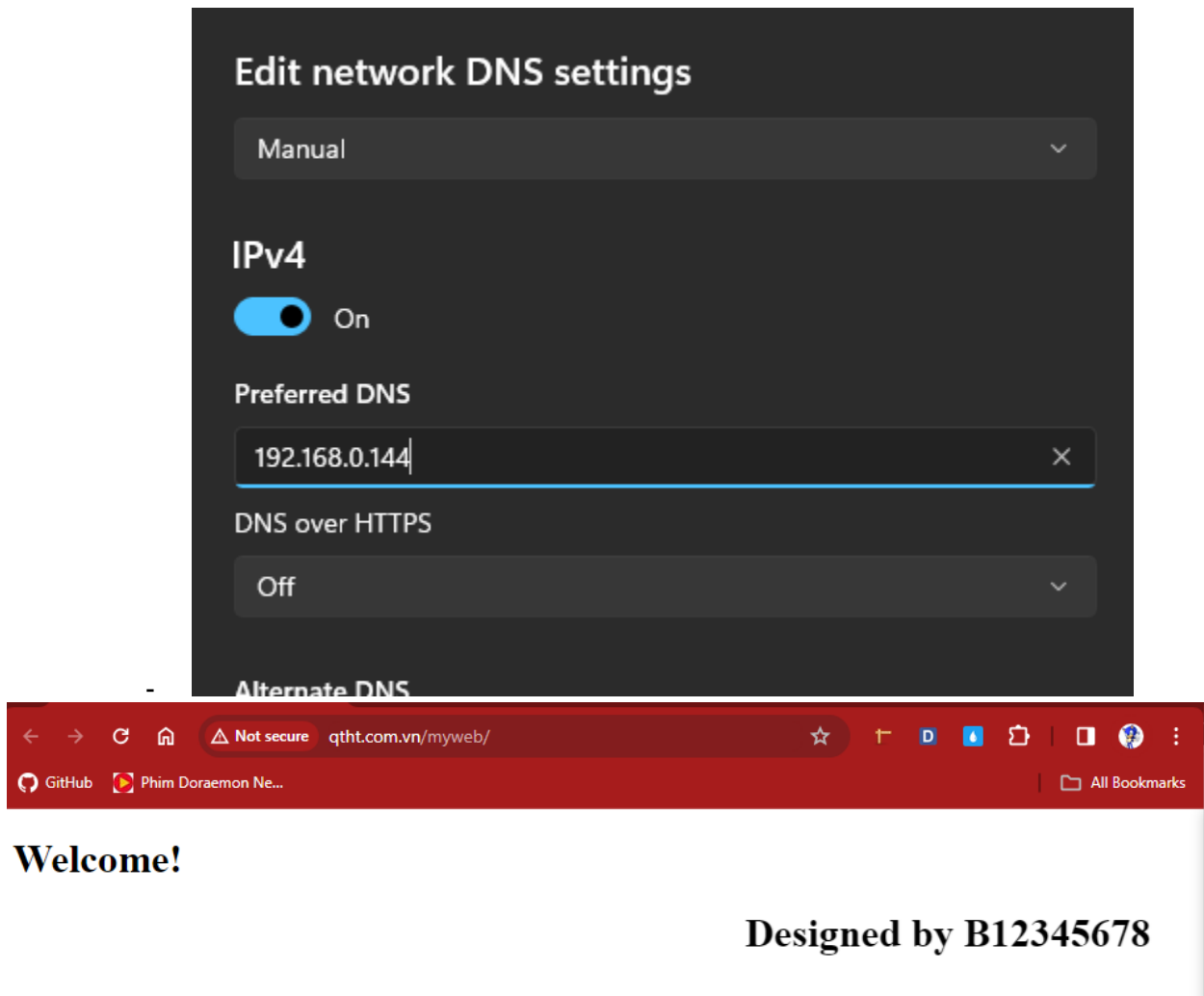
Name:   htql.qtht.com.vn
Address: 8.8.8.8

[b2110072@server1 data]$ nslookup www.ctu.edu.vn 192.168.0.144
Server:          192.168.0.144
Address:         192.168.0.144#53

Non-authoritative answer:
Name:   www.ctu.edu.vn
Address: 123.30.143.225

[b2110072@server1 data]$
```

- 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>



4. Cấu hình tường lửa FirewallD

Công cụ FirewallD (dynamic firewall daemon) cung cấp dịch vụ tường lửa mạnh mẽ, toàn diện; được cài đặt mặc định cho nhiều bản phân phối Linux. Từ CentOS 7 trở về sau, tường lửa FirewallD được thay thế cho tường lửa iptables với những khác biệt cơ bản:

- FirewallD sử dụng “zone” như là một nhóm các quy tắc (rule) áp đặt lên những luồng dữ liệu. Một số zone có sẵn thường dùng:
 - *drop*: ít tin cậy nhất – toàn bộ các kết nối đến sẽ bị từ chối.
 - *public*: đại diện cho mạng công cộng, không đáng tin cậy. Các máy tính/services khác không được tin tưởng trong hệ thống nhưng vẫn cho phép các kết nối đến tùy từng trường hợp cụ thể.
 - *trusted*: đáng tin cậy nhất – tin tưởng toàn bộ thiết bị trong hệ thống.
- FirewallD quản lý các quy tắc được thiết lập tự động, có tác dụng ngay lập tức mà không làm mất đi các kết nối và session hiện có.
 - *Runtime* (mặc định): có tác dụng ngay lập tức nhưng mất hiệu lực khi reboot hệ thống.

- *Permanent*: không áp dụng cho hệ thống đang chạy, cần reload mới có hiệu lực, tác dụng vĩnh viễn cả khi reboot hệ thống.

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

- Khởi động tường lửa firewalld
\$sudo systemctl start firewalld

```
b2110072@server1:~ — sudo systemctl status firewalld
[b2110072@server1 ~]$ sudo systemctl start firewalld
[sudo] password for b2110072:
[b2110072@server1 ~]$ sudo systemctl status firewalld
• firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
  Active: active (running) since Wed 2024-04-10 22:23:31 +07; 4s ago
    Docs: man:firewalld(1)
   Main PID: 51959 (firewalld)
     Tasks: 2 (limit: 17255)
    Memory: 29.2M
       CPU: 308ms
    CGroup: /system.slice/firewalld.service
           └─51959 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid

Apr 10 22:23:31 server1 systemd[1]: Starting firewalld - dynamic firewall daemon>
Apr 10 22:23:31 server1 systemd[1]: Started firewalld - dynamic firewall daemon.
lines 1-13/13 (END)
```

- Liệt kê tất cả các zone đang có trong hệ thống
\$firewall-cmd --get-zones

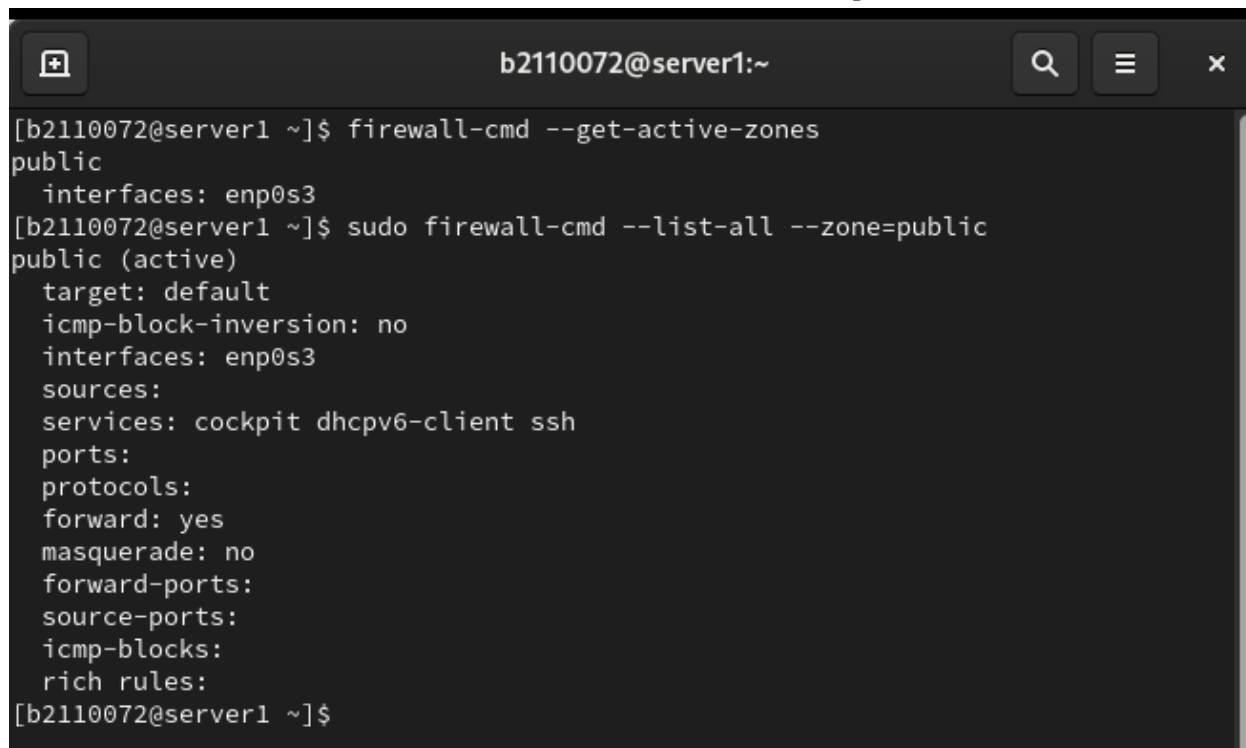
```
b2110072@server1:~
[b2110072@server1 ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[b2110072@server1 ~]$
```

- Kiểm tra zone mặc định
\$firewall-cmd --get-default-zone

```
b2110072@server1:~
[b2110072@server1 ~]$ firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
[b2110072@server1 ~]$ firewall-cmd --get-default-zone
public
[b2110072@server1 ~]$
```

- Kiểm tra zone đang được sử dụng bởi giao diện mạng (thường là *public*); và xem các rules của zone

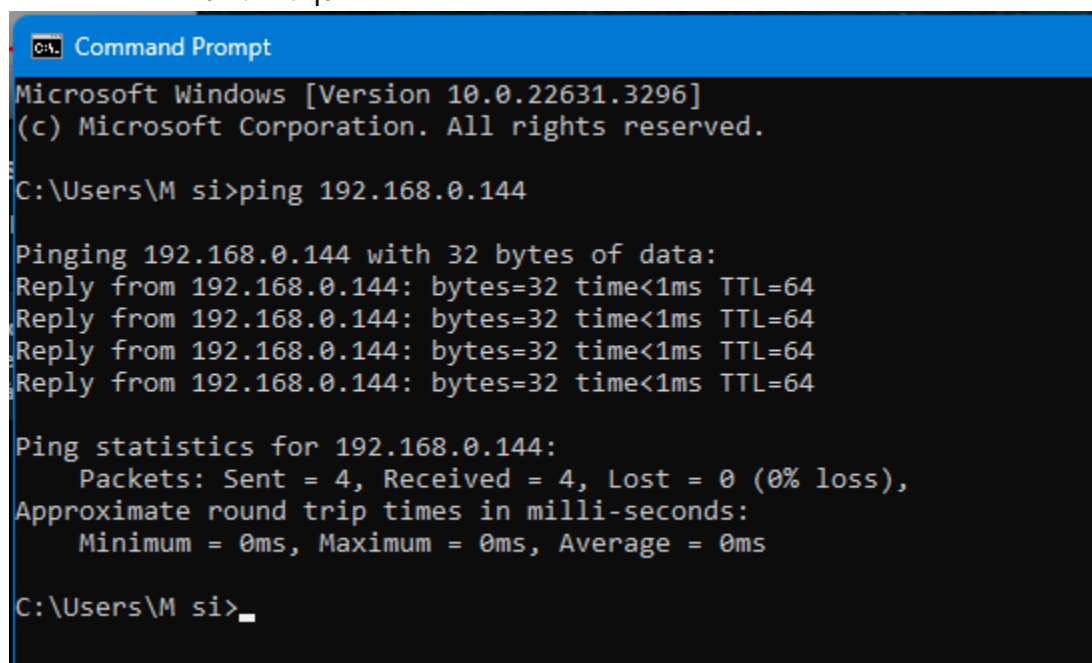
```
$firewall-cmd --get-active-zones
$sudo firewall-cmd --list-all --zone=public
```



A terminal window titled 'b2110072@server1:~' with search, menu, and close icons. It shows the execution of two firewall commands. The first command, 'firewall-cmd --get-active-zones', returns 'public' and lists the active interface 'enp0s3'. The second command, 'sudo firewall-cmd --list-all --zone=public', shows the configuration for the 'public' zone, including target, interfaces, services, ports, protocols, and rules.

```
[b2110072@server1 ~]$ firewall-cmd --get-active-zones
public
  interfaces: enp0s3
[b2110072@server1 ~]$ sudo firewall-cmd --list-all --zone=public
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[b2110072@server1 ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.



A Windows Command Prompt window titled 'Command Prompt' showing the execution of a ping command to 192.168.0.144. The output shows four successful replies with 0% loss and 0ms round trip times.

```
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\M si>ping 192.168.0.144

Pinging 192.168.0.144 with 32 bytes of data:
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\M si>
```

- Chuyển giao diện mạng sang zone *drop*; và xem các rules của zone
\$sudo firewall-cmd --zone=drop --change-interface=enp0s3
\$sudo firewall-cmd --list-all --zone=drop

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo firewall-cmd --list-all --zone=drop
drop
  target: DROP
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[b2110072@server1 ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.
- Chuyển giao diện mạng sang zone *trusted*; và xem các rules của zone
\$sudo firewall-cmd --zone=trusted --change-interface=enp0s3
\$sudo firewall-cmd --list-all --zone=trusted

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo firewall-cmd --zone=trusted --change-interface=enp0s3
success
[b2110072@server1 ~]$ sudo firewall-cmd --list-all --zone=trusted
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services:
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[b2110072@server1 ~]$
```

- Từ máy vật lý, ping, truy cập dịch vụ web và kết nối SSH tới máy CentOS. Cho biết kết quả.

```
Command Prompt
Microsoft Windows [Version 10.0.22631.3296]
(c) Microsoft Corporation. All rights reserved.

C:\Users\M si>ping 192.168.0.144

Pinging 192.168.0.144 with 32 bytes of data:
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64
Reply from 192.168.0.144: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

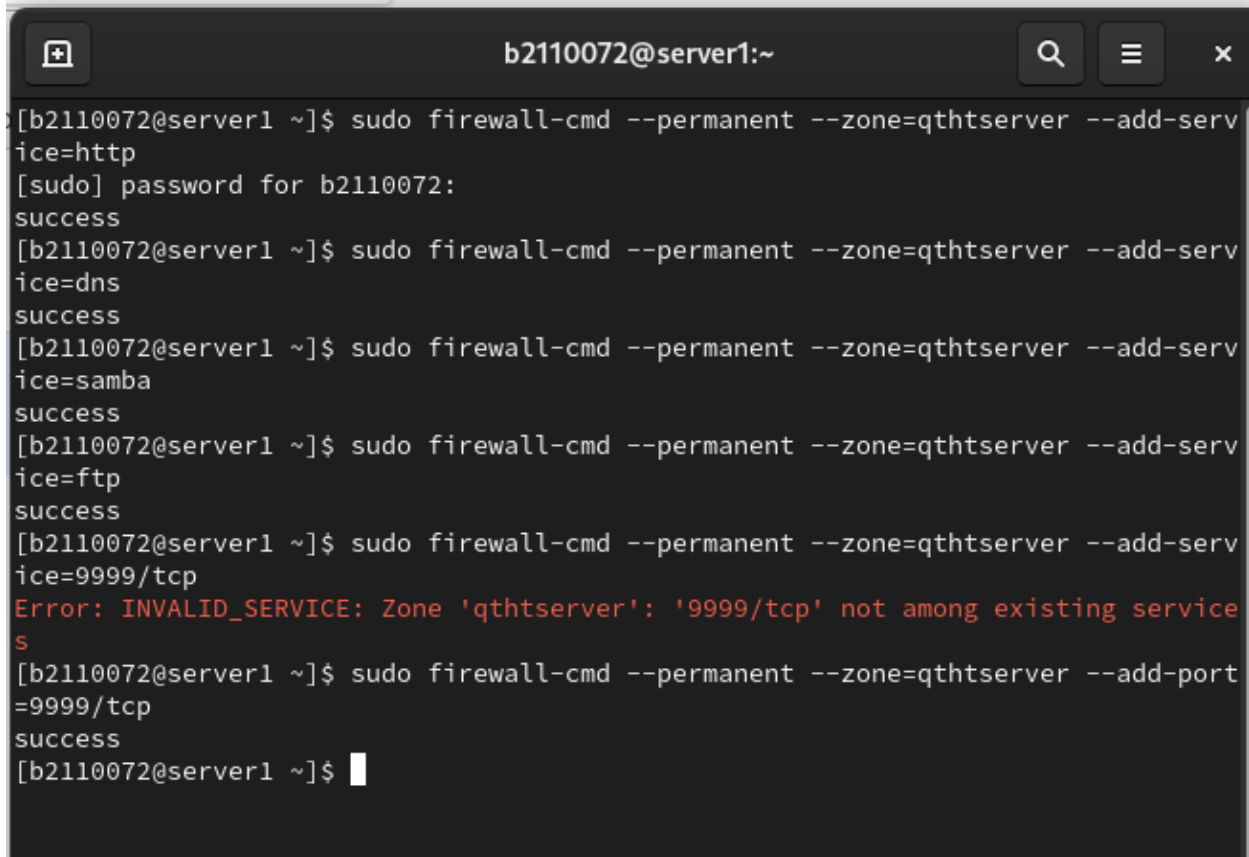
C:\Users\M si>
```

- Tạo zone mới có tên là *qthtserver*
\$sudo firewall-cmd --permanent --new-zone=qthtserver
\$sudo systemctl restart firewalld
\$sudo firewall-cmd --list-all --zone=qthtserver

```
b2110072@server1:~
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --new-zone=qthtserver
[sudo] password for b2110072:
success
[b2110072@server1 ~]$ sudo systemctl restart firewalld
[b2110072@server1 ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services:
  ports:
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[b2110072@server1 ~]$
```

- Cho phép các dịch vụ HTTP, DNS, SAMBA, FTP và cổng 9999/tcp hoạt động trên zone *qthtserver*

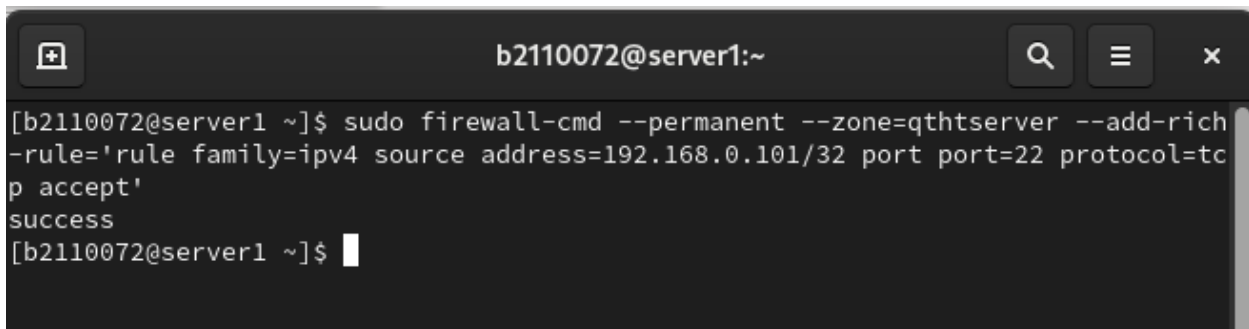
```
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
$sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
$sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
```



A terminal window titled 'b2110072@server1:~' showing the execution of firewall commands. The user runs 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=http', 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns', 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba', and 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp', all of which succeed. Then, the user runs 'sudo firewall-cmd --permanent --zone=qthtserver --add-service=9999/tcp', which fails with the error 'INVALID_SERVICE: Zone 'qthtserver': '9999/tcp' not among existing services'. Finally, the user runs 'sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp', which succeeds.

```
b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=http
[sudo] password for b2110072:
success
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=dns
success
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=samba
success
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=ftp
success
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-service=9999/tcp
Error: INVALID_SERVICE: Zone 'qthtserver': '9999/tcp' not among existing services
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-port=9999/tcp
success
[b2110072@server1 ~]$
```

- Thêm rule để chỉ cho phép máy vật lý có thể SSH tới máy CentOS
\$sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=<IP máy vật lý>/32 port port=22 protocol=tcp accept'

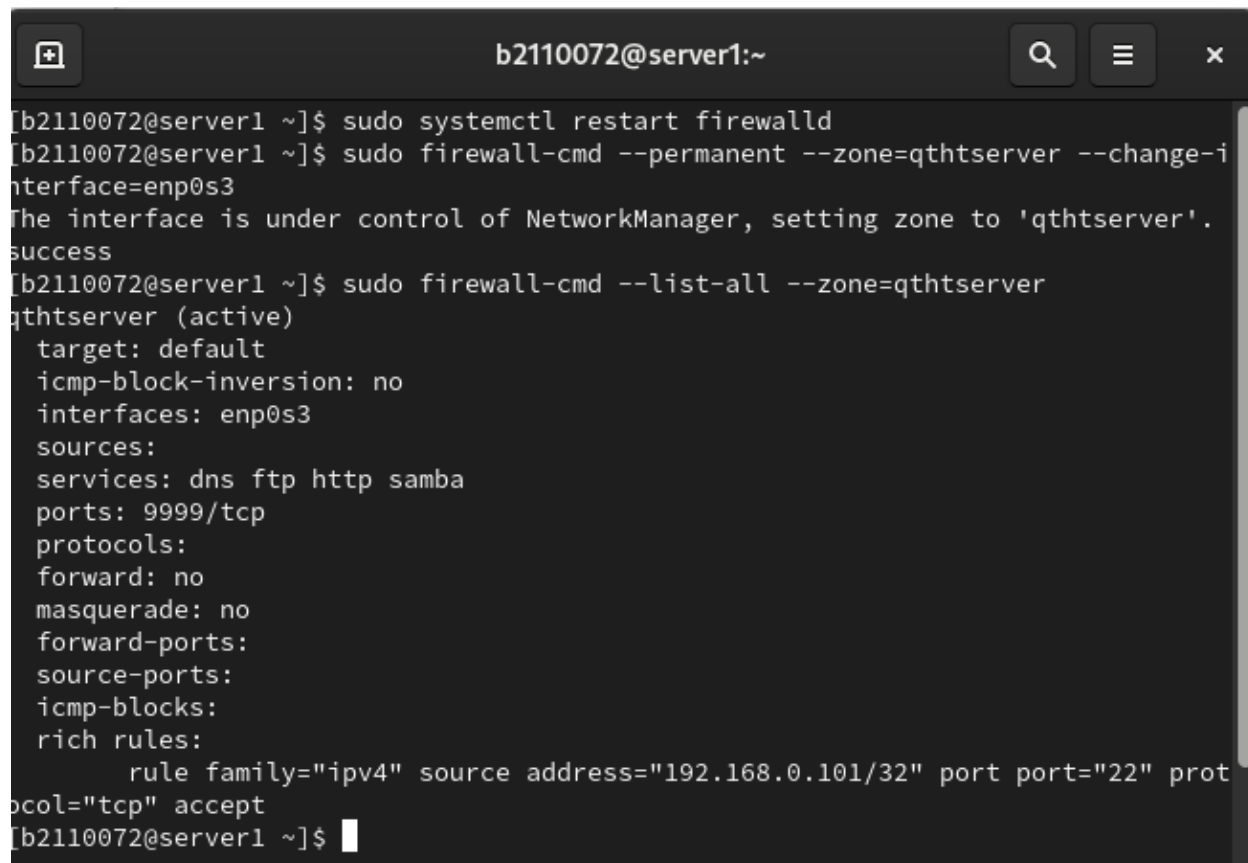


A terminal window titled 'b2110072@server1:~' showing the execution of a firewall command. The user runs 'sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.0.101/32 port port=22 protocol=tcp accept'', which succeeds.

```
b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --add-rich-rule='rule family=ipv4 source address=192.168.0.101/32 port port=22 protocol=tcp accept'
success
[b2110072@server1 ~]$
```

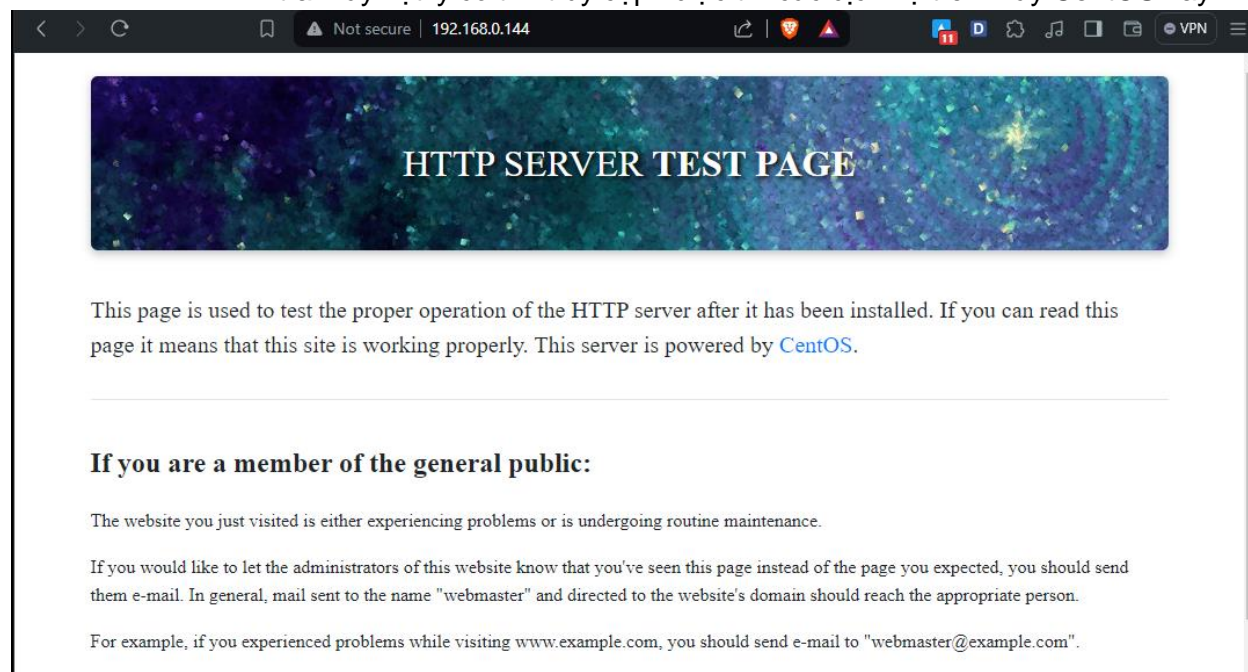
- Khởi động lại tường lửa firewallld
\$sudo systemctl restart firewallld
- Chuyển giao diện mạng sang zone qthtserver; và xem các rules của zone

```
$sudo firewall-cmd --permanent --zone=qthtserver --change-interface=enp0s3
$sudo firewall-cmd --list-all --zone=qthtserver
```



```
b2110072@server1:~
[b2110072@server1 ~]$ sudo systemctl restart firewalld
[b2110072@server1 ~]$ sudo firewall-cmd --permanent --zone=qthtserver --change-i
nterface=enp0s3
The interface is under control of NetworkManager, setting zone to 'qthtserver'.
success
[b2110072@server1 ~]$ sudo firewall-cmd --list-all --zone=qthtserver
qthtserver (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: dns ftp http samba
  ports: 9999/tcp
  protocols:
  forward: no
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv4" source address="192.168.0.101/32" port port="22" prot
ocol="tcp" accept
[b2110072@server1 ~]$
```

- Kiểm tra máy vật lý có thể truy cập được tới các dịch vụ trên máy CentOS hay không.



--- Hết ---

Video hướng dẫn làm bài:

- + Hướng dẫn làm bài: <https://youtu.be/MgrW8zeh02E>
- + Hướng dẫn câu 1: <https://youtu.be/0oW0TF1iVQs>
- + Hướng dẫn câu 2: <https://youtu.be/ZuRg100dtJQ>
- + Hướng dẫn câu 3: https://youtu.be/89mAL_T_uuY
- + Hướng dẫn câu 4: <https://youtu.be/cS3Qv90bBQ8>