ĐH Khoa Học Tự Nhiên TP.HCM

Khoa Mạng Máy Tính

Bộ môn Chuyên đề Hệ điều hành Linux

BÁO CÁO ĐỒ ÁN THỰC HÀNH CUỐI KỲ

Học kỳ 1 - năm học 2018-2019

# Danh sách thành viên

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | MSSV | Họ và tên | Email | Số điện thoại |
| 1 | 1312663 | Nguyễn Minh Tuấn | [nmtuan.dev@gmail.com](mailto:nmtuan.dev@gmail.com) | 0934018329 |

Link phần bài nộp video: <https://drive.google.com/open?id=1g2_hY3vXTbV34G2xxkSm7OK9ApegXzlS>

# Kết quả hoàn thành

Mức độ hoàn thành dự tính: 90%

✅ Thiết kế network, phân chia subnet

✅ Cấu hình dịch vụ DHCP

✅ Cấu hình dịch vụ DNS

✅ Cấu hình dịch vụ Web

✅ Static Website

✅ Dynamic filesystem directory listing

✅ Basic Auth

✅ Cấu hình dịch vụ SSH/SFTP

✅ Cấu hình firewall/router/http-proxy

✅ Cấu hình sample user host

❌ Cấu hình mail server

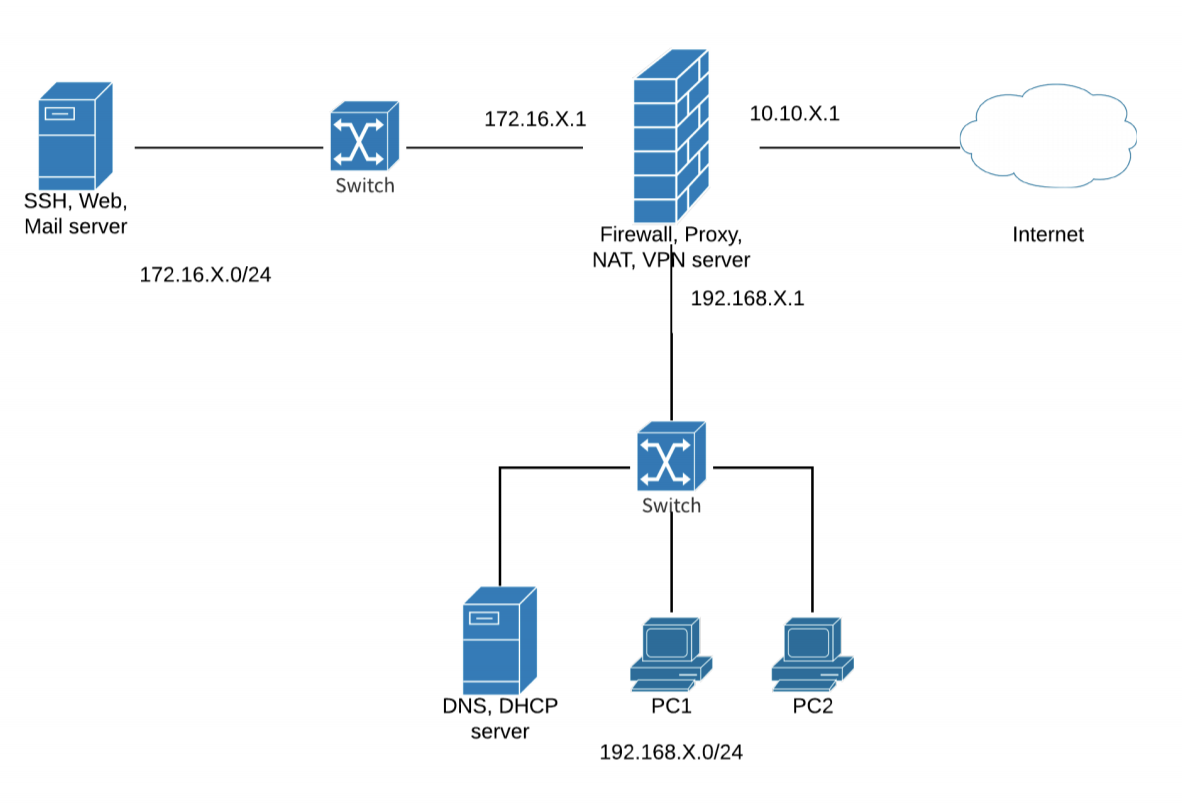
# Lựa chọn công nghệ

Sau khi nghiên cứu và thử nghiệm nhóm em quyết định chọn Docker và Docker Compose làm công nghệ để thực hiện đồ án thực hành này.

# Tổng quan về kiến trúc

Kiến trúc mạng của nhóm em thiết kế khá giống với yêu cầu đồ án đưa ra. Kiến trúc này gồm 2 subnet chính: Intranet và DMZ

Ngoài ra nhóm em còn thêm vào subnet Extranet để giả lập access đến từ bên ngoài.

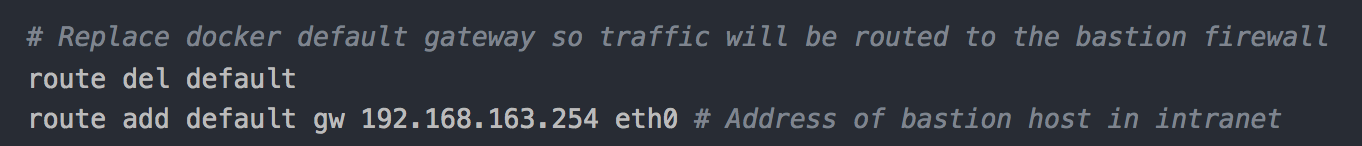


Các subnet này được kết nối với nhau qua một bastion host. Bastion host này được cấu hình đồng thời như router, firewall và transparent HTTP proxy.

# Cấu hình cụ thể

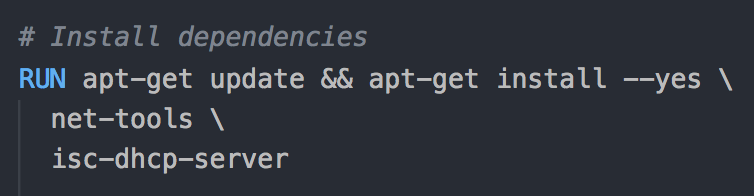
Toàn bộ các host trong bài thực hành này đều được chúng em cấu hình trên nền tảng Ubuntu 18.04 Docker container.

Ngoài ra Docker cũng tồn tại một số hạn chế như không thể khai báo default gw trên file compose. Để giải quyết chuyện này chúng em đã cài đặt bộ phần mềm net-tools và override default gw ở các host (trong Intranet và DMZ) để chúng trỏ tới Bastion host

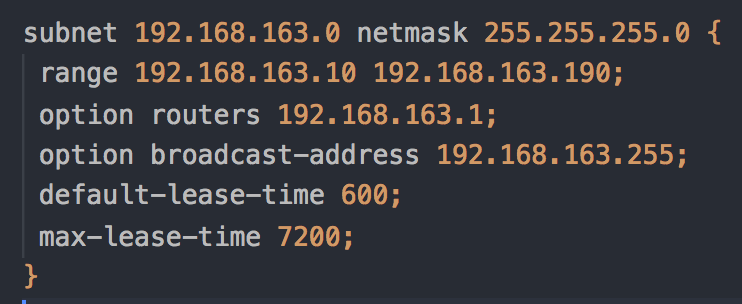


## Cấu hình DHCP Host

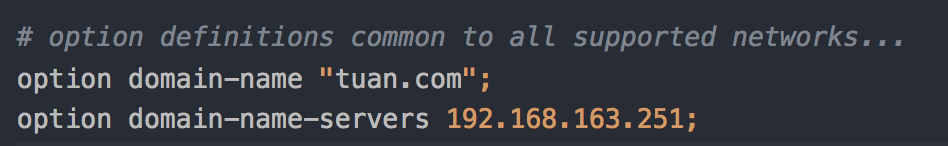
Để cái đặt DHCP host trên ubuntu thì chúng em phải cài gói phần mềm **isc-dhcp-server**



Đề cấu hình dịch vụ DHCP thì chúng em phải chỉnh sửa nội dung của file **/etc/dhcp/dhcpd.conf**. Vì DHCP server này chỉ cần phục vụ cho các máy của user trong Intranet nên chúng em chỉ cần config cho duy nhất một subnet tương ứng

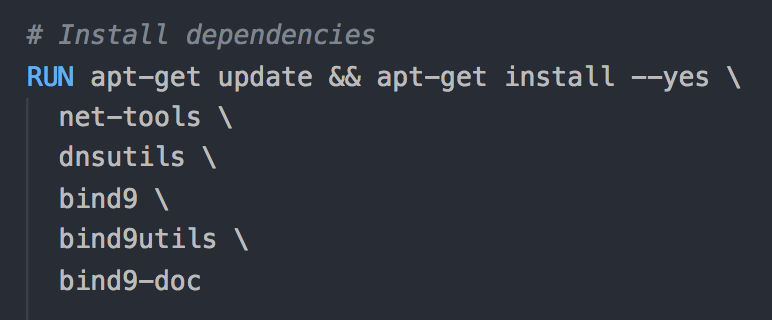


Ngoài ra cấu hình default DNS server cũng được bọn em đặt trong file **/etc/dhcp/dhcpd.conf**

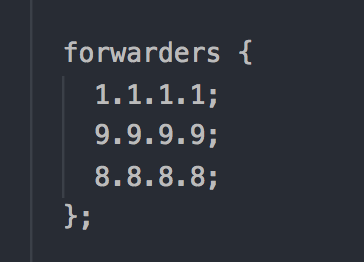


## DNS Host

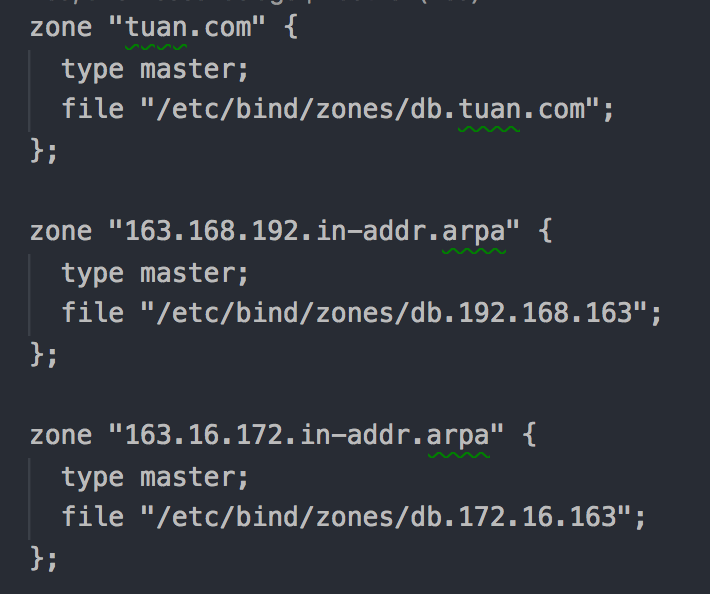
Để cầu hình DNS host trên Ubuntu thì chúng em phải cài đặt các gói phần mềm bind.



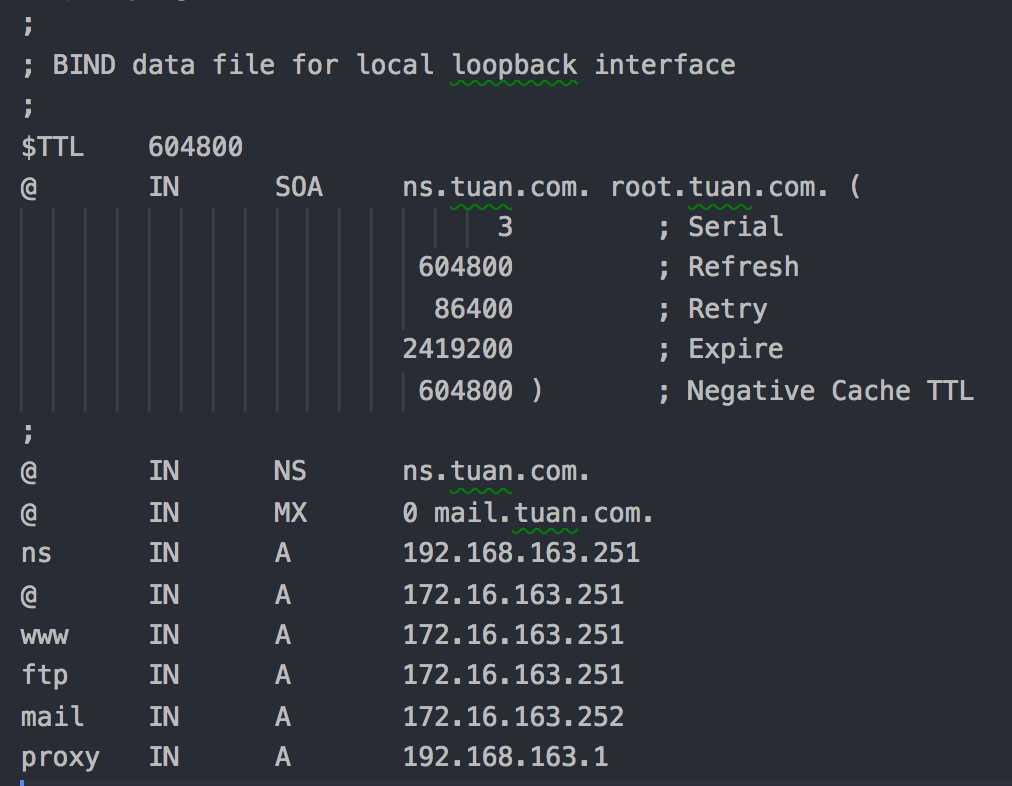
Đầu tiên chúng em phải cấu hình file **/etc/bind/named.conf.options** để khai báo các forwarder server tương ứng nếu DNS record không được tìm thấy.



Sau đó chúng em phải cấu hình file **/etc/bind/named.conf.local** để khai báo các DNS zone và các file database tương ứng của chúng. Ngoài zone chính cho domain của nhóm thì chúng em cũng khai báo các reverse lookup zone tương ứng với các subnet



Với mỗi zone thì chúng em sẽ phải cấu hình DNS record tương ứng trong file database đã được khai báo. Ví dụ file database của zone “tuan.com” ở **/etc/bind/zones/db.tuan.com**



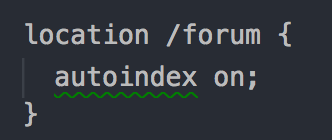
## Web Host

Web host mà chúng em cầu hình gồm có 2 phần chính  
- NGINX server để phục vụ HTTP/HTTPS traffic.

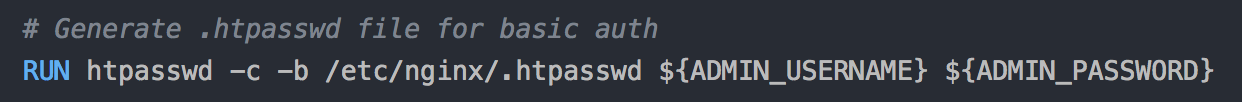
- OpenSSH server để administrator có thể login và cấu hình các static file tương ứng

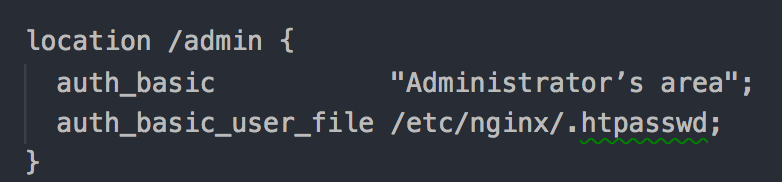
Để cấu hình NGINX thì trước hết chung em phải cài đặt gói phần mềm nginx. Sau đó chúng em phải chuẩn bị static web directory ở **/var/www/tuan.com** và nhúng cấu hình server tương ứng ở **/etc/nginx/sites-available/tuan.com**, symlink vào **/etc/nginx/sites-enabled/tuan.com** để enable site.

Đối với yêu cầu list file directory thì chúng em sử dụng tính năng autoindex của NGINX để hiện thị webpage như một filesystem directory



Đối với yêu cầu basic auth route thì trước tiên chúng em phải generate ra file .htpasswd cho admin user bằng công cụ **htpasswd** trong gói phần mềm **apache2-utils**. File này được đặt ở **/etc/nginx/.htpasswd** và sẽ được cấu hình để NGINX sử dụng làm basic auth database file





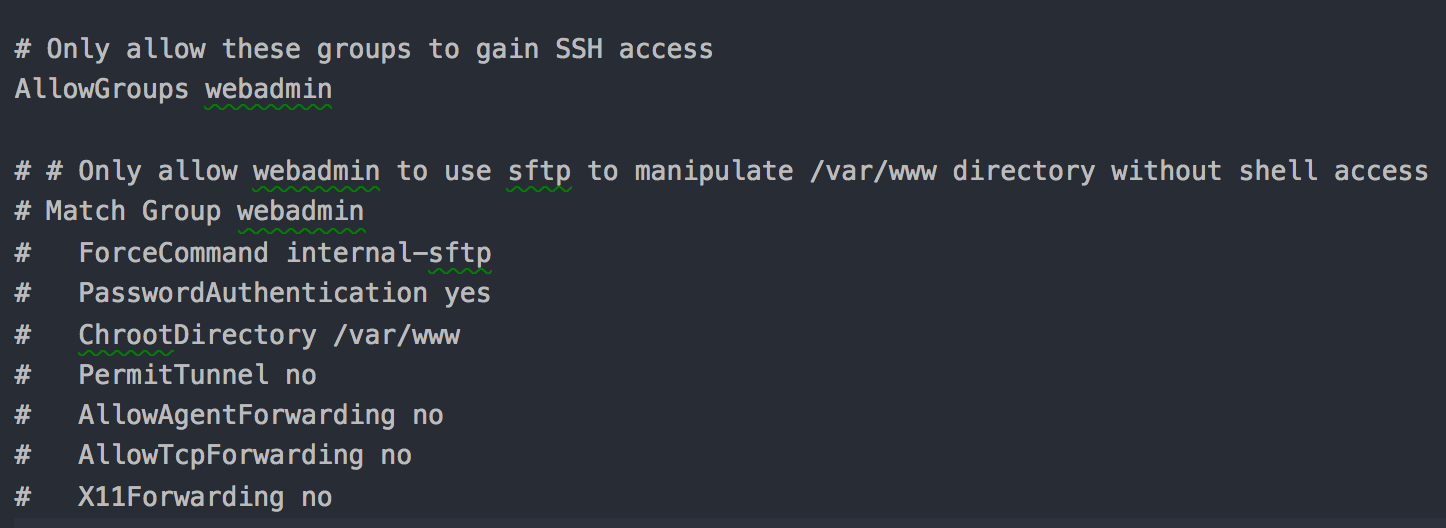
Để setup SSL, ở đây chúng em chỉ sử dụng self-signed cert, đầu tiên chúng em phải generate ra cặp SSL key và cert bằng công cụ openssl

openssl req -x509 -nodes -days 3650 -newkey rsa:4096 -keyout site.key -out site.crt

Sau đó em phải cấu hình để NGINX phục vụ SSL traffic với cặp key và cert trên

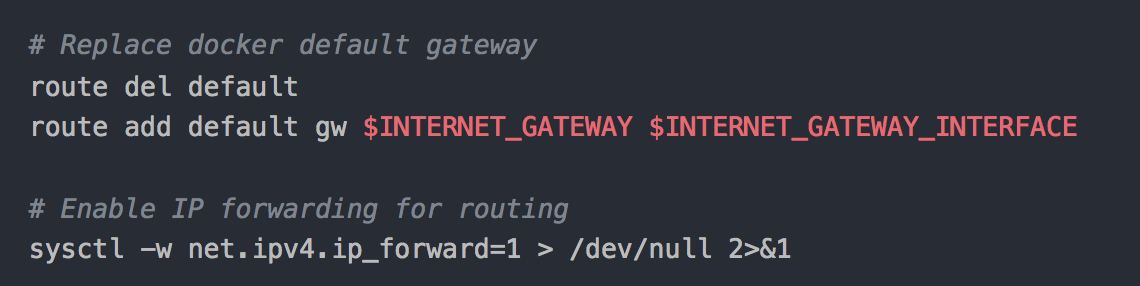


Để cấu hình dịch vụ SSH, thì chúng em phải cài gói phần mềm **openssh-server**. Và cấu hình file **/etc/ssh/sshd\_config** theo yêu cầu của đề bài (PermitRootLogin no, …) Ngoài ra em cũng có cấu hình chỉ cho phép user SFTP lên thư mục **/var/www** và cấm shell access. Tuy nhiên để dễ test thì em comment phần này ra.

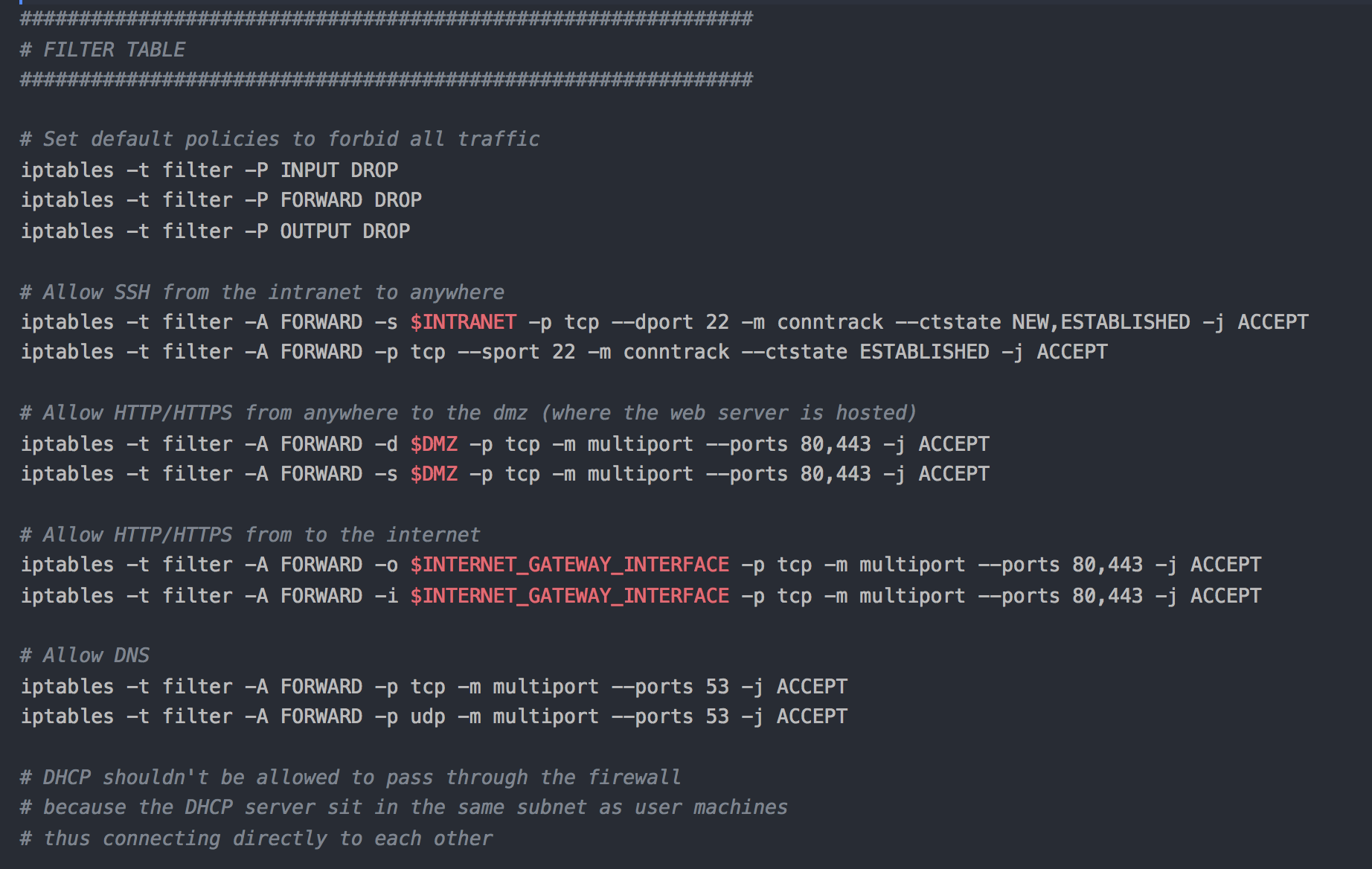


## Bastion Host

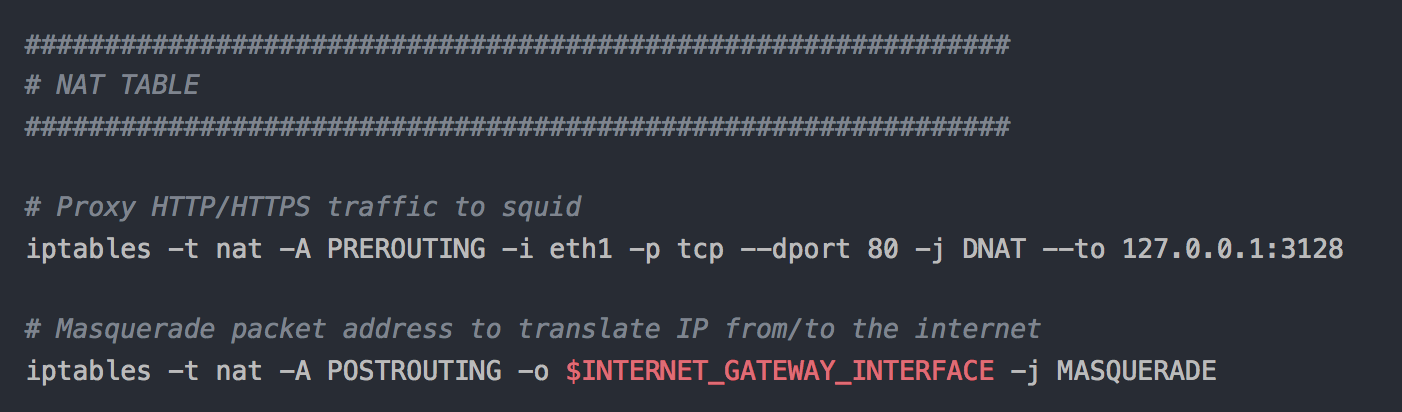
Để cấu hình bastion host này đầu tiên chúng em phải cấu hình cho nó trở thành một network router. Với gói phần mềm net-tools chúng em có thể chỉnh sửa route table ở dưới Linux kernel. Ngoài ra chúng em còn phải enable kernal IP forwarding bằng lệnh **sysctl**



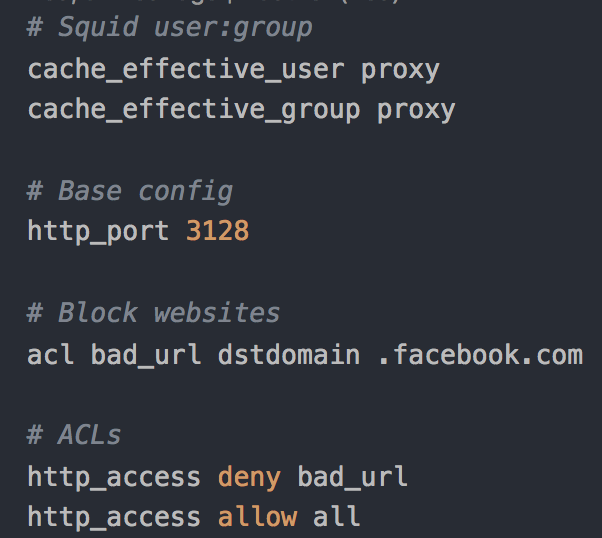
Về firewall thì chúng em sử dụng công cụ iptables để cấu hình network như yêu cầu đồ án



Để các máy trong mạng intranet có thể access được internet thì em cũng config các NAT rule tương ứng. Ngoài ra chúng em còn sử dụng và cấu hình Squid làm transparent HTTP proxy. Chúng em phải route các gói HTTP packet qua Squid server chạy chung với bastion host

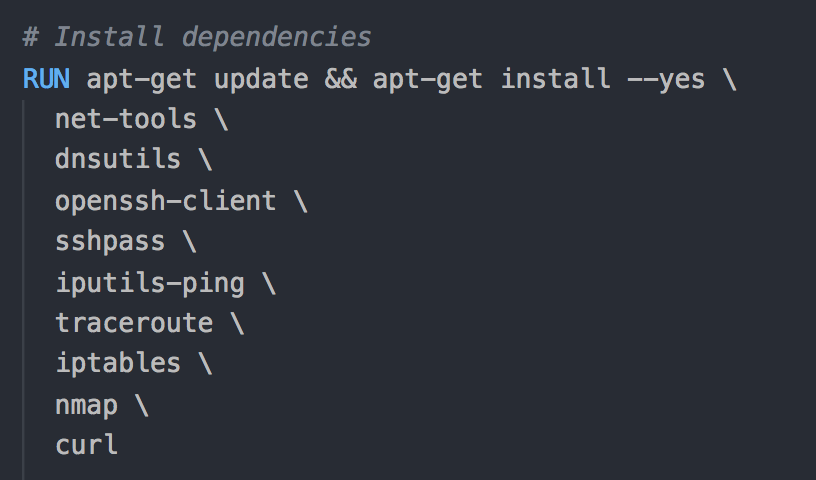


Cấu hình squid tại **/etc/squid/squid.conf**



## User Host

Để cấu hình user host thì phần lớn chúng em phải cài các gói client phù hợp để tương tác với các dịch vụ.



Ví dụ như gói nmap để gửi gói tin DHCP broadcast, gói dnsutils để kiểm tra DNS server, gói openssh client để kiểm tra cầu hình SSH…

Các script thực hiện cụ thể việc kiểm tra này được em đặt trong source code nộp kèm

# Bảng phân công công việc

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Miêu tả công việc | Thành viên thực hiện | Phần trăm công việc |
| 1 | Nghiên cứu kiến trúc và lựa chọn công nghệ | 1312663 | 10% |
| 2 | Cấu hình git và github repository | 1312663 | 5% |
| 3 | Cấu hình hệ thống mạng và phân chia subnet | 1312663 | 15% |
| 4 | Cấu hình dịch vụ DHCP | 1312663 | 10% |
| 5 | Cấu hình dịch vụ DNS | 1312663 | 10% |
| 6 | Cấu hình dịch vụ Web NGINX và SSH | 1312663 | 20% |
| 7 | Cấu hình Bastion host routing/firewall/squid proxy | 1312663 | 20% |
| 8 | Soạn tài liệu và viết báo cáo | 1312663 | 10% |

Tổng phân công:

1312663 - 100%