Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

5

Lab

Khai thác tường lửa trong Linux

Thực hành môn An toàn mạng

Tháng 9/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Tìm hiểu cách thức hoạt động của tường lửa và thực hiện triển khai tường lửa đơn giản.

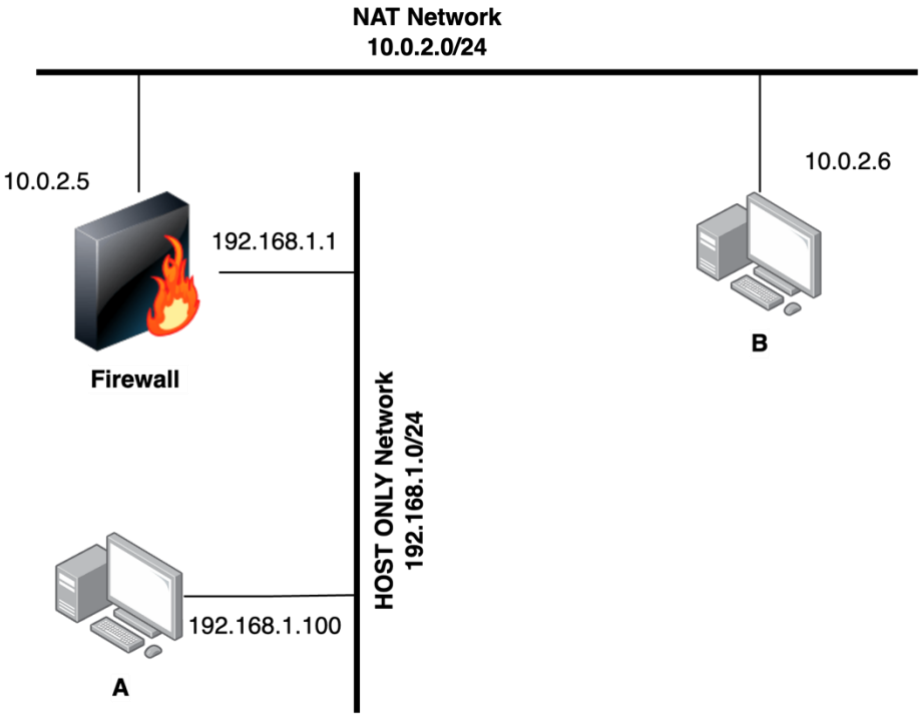
2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Cài đặt 2 máy ảo Ubuntu (có thể sử dụng Seed Ubuntu 20.04 hoặc các máy ảo đã có sẵn từ các bài thực hành trước)
- Tải và cài đặt Pfsense theo hướng dẫn ở mục 1.
- Cấu hình network cho các máy ảo theo mô hình mạng ở hình 1.

C. THỰC HÀNH



Hình 1. Mô hình mạng bài thực hành

1. Cài đặt PfSense

Sinh viên tải về file cài đặt pfsense với bản cài CD Image (iso) Installer từ trang web https://www.pfsense.org/download/. Sau khi tải về, tiến hành giải nén (.gz) để được file .iso và thực hiện cài đặt máy ảo.

Tạo máy ảo có các thông số sau:

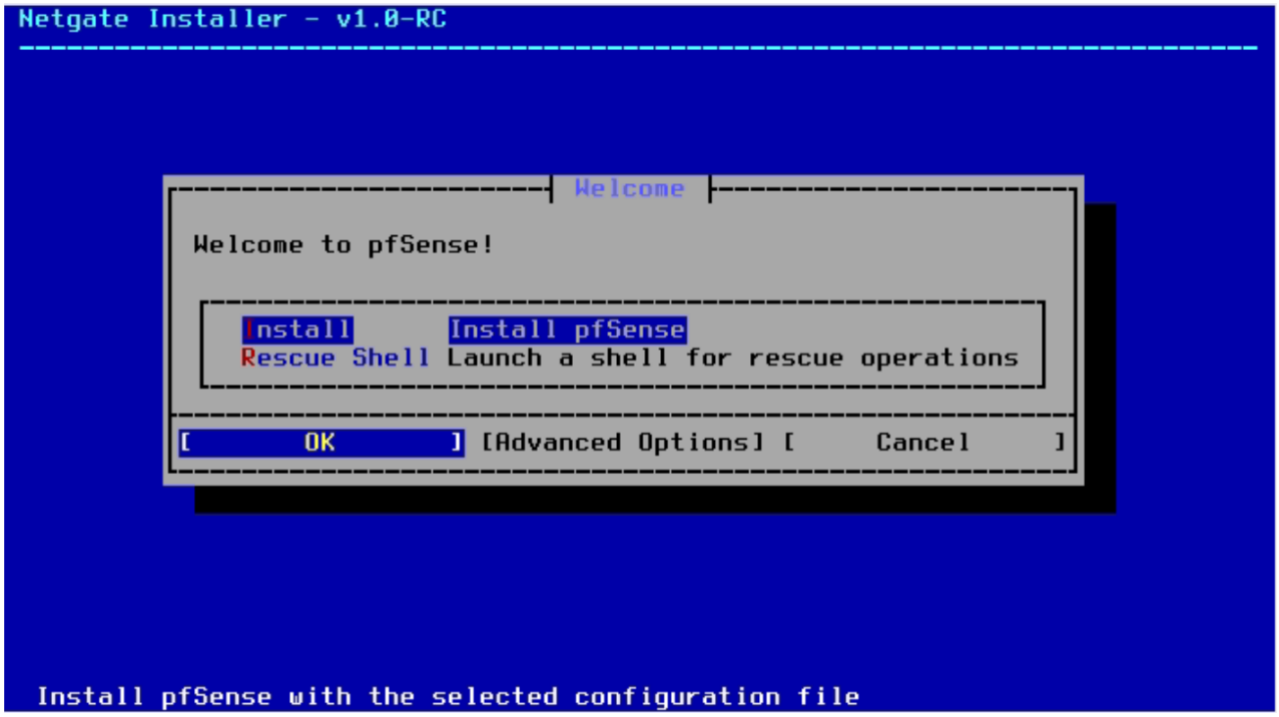
- Hệ điều hành: Linux 4.x kernel trở lên
- Loại Firmware: Legacy BIOS
- Network: Tạo 2 card mạng (NAT và Host only)

a. Cài đặt Pfsense

Tải về file cài đặt pfsense phiên bản iso từ trang web https://www.pfsense.org/download/. Sau khi tải về, tiến hành giải nén và thực hiện cài đặt máy ảo với file iso.

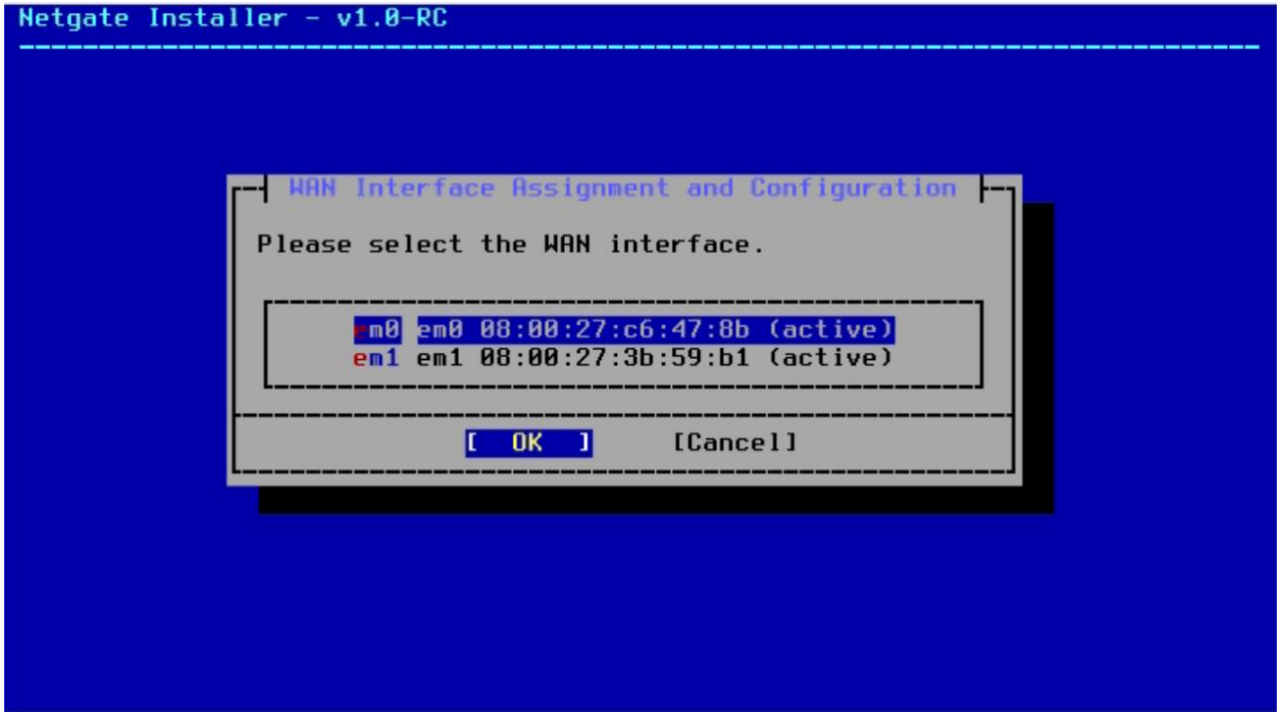
Bước 1: Khởi động máy ảo từ file iso

Bước 2: Chọn Install pfsense

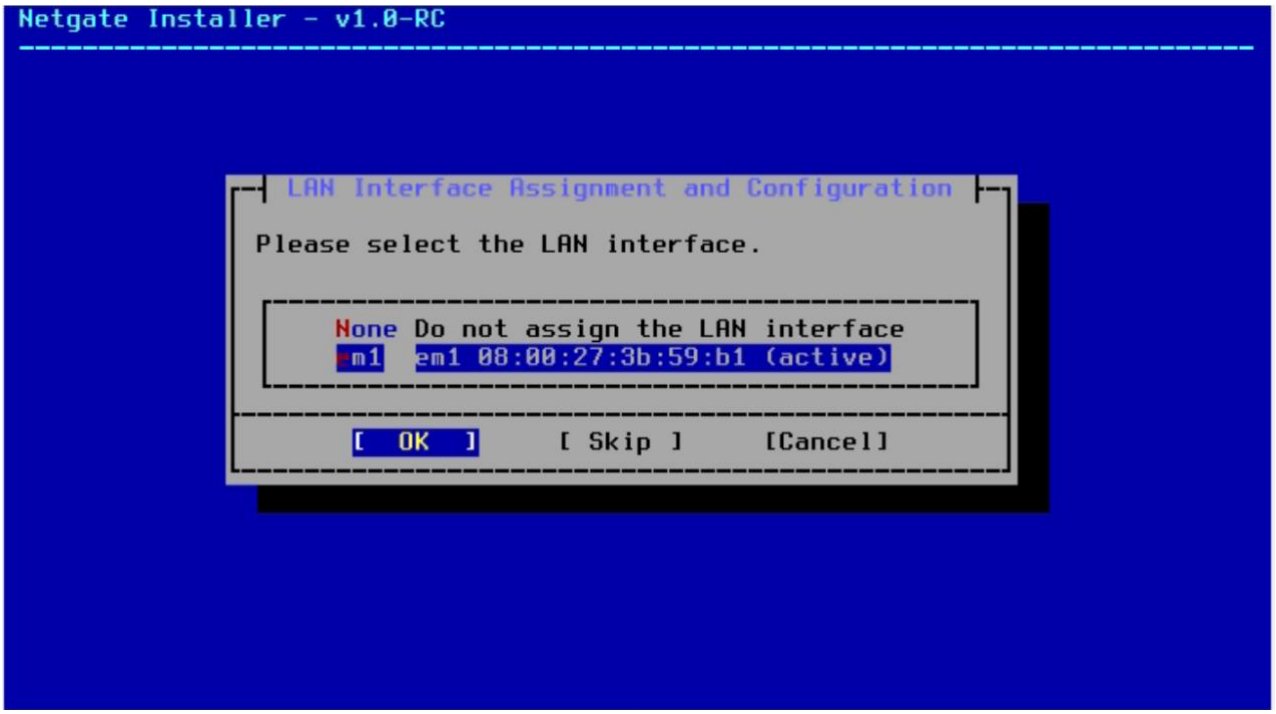


Hình 2 Cài đặt pfsense

Bước 3: Cấu hình các card mạng. Hệ thống pfSense thông thường sẽ sử dụng 2 card mạng. Trong đó, WAN interface sẽ gắn với card NAT; LAN interface sẽ được gắn với card Host Only. Chúng ta sẽ dựa vào MAC Address để chọn đúng các card mạng.

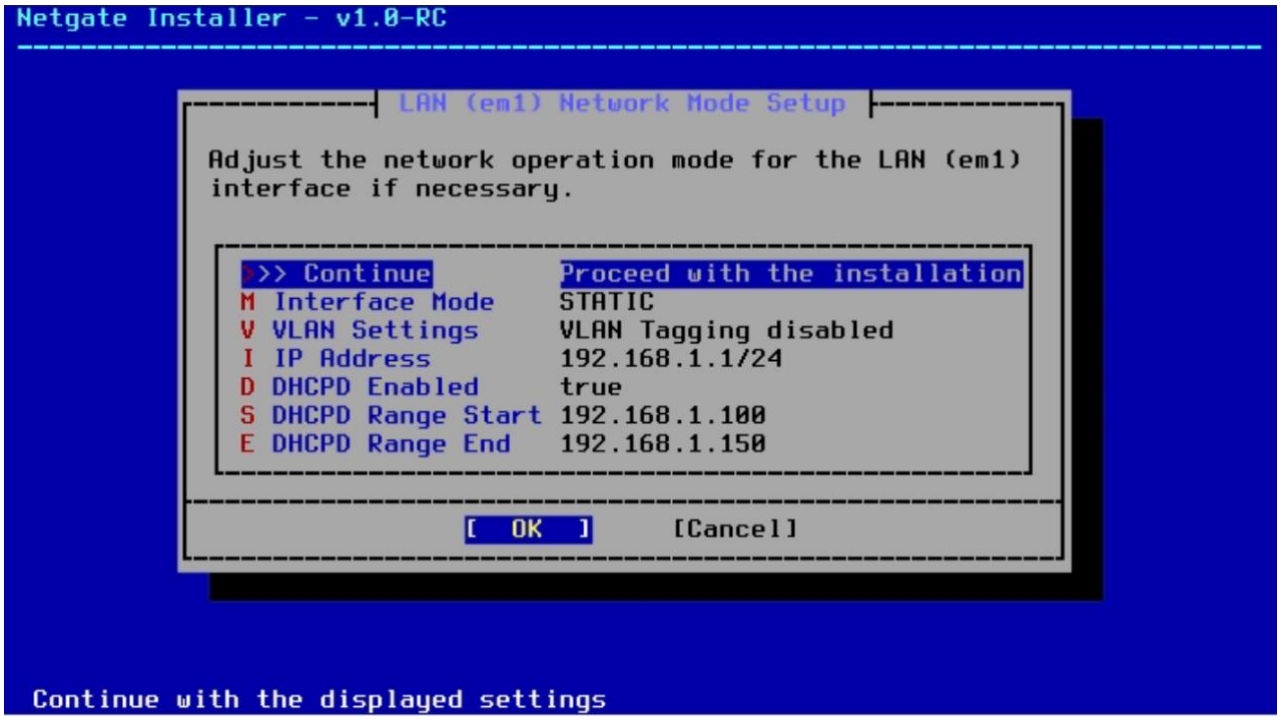


Hình 3 Lựa chọn card mạng WAN



Hình 4 Lựa chọn card mạng LAN

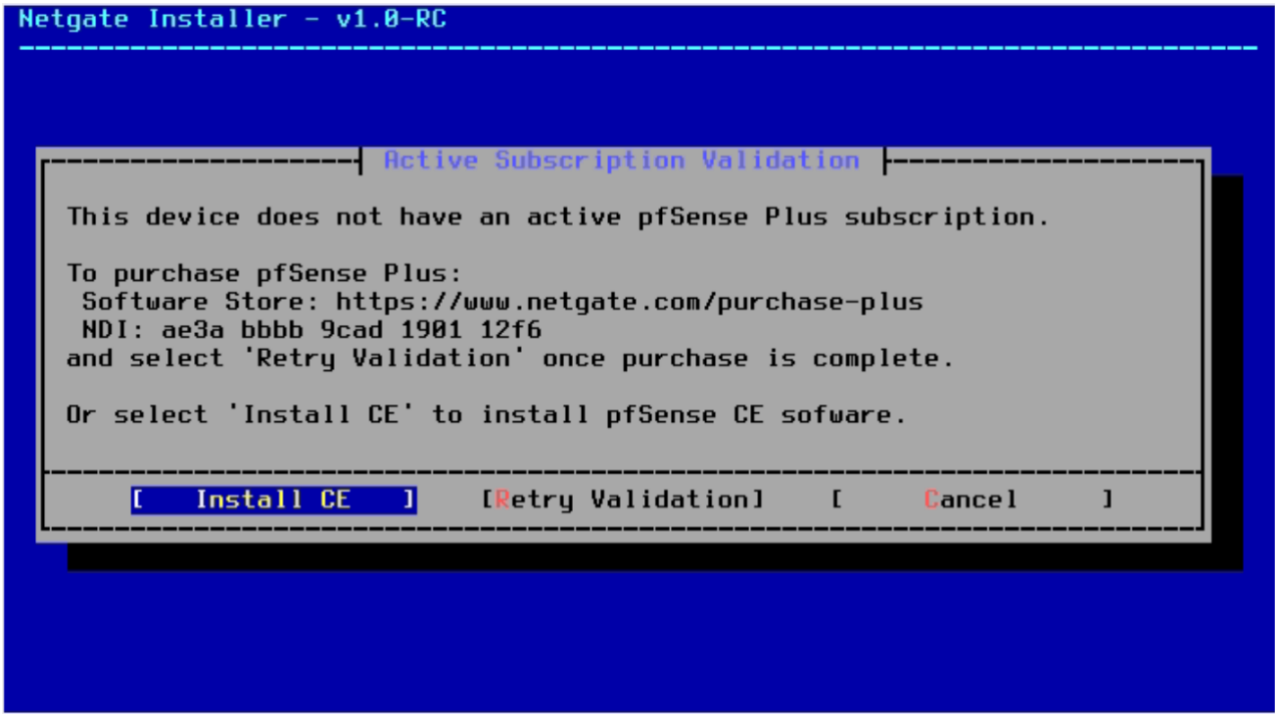
Bước 4: Đối với mạng LAN, chúng ta có thể đặt lại địa chỉ IP cho interface này.



Hình 5 Cấu hình IP cho mạng LAN

Sau khi cấu hình xong địa chỉ IP, xác nhận lại các thông tin và tiếp tục cài đặt.

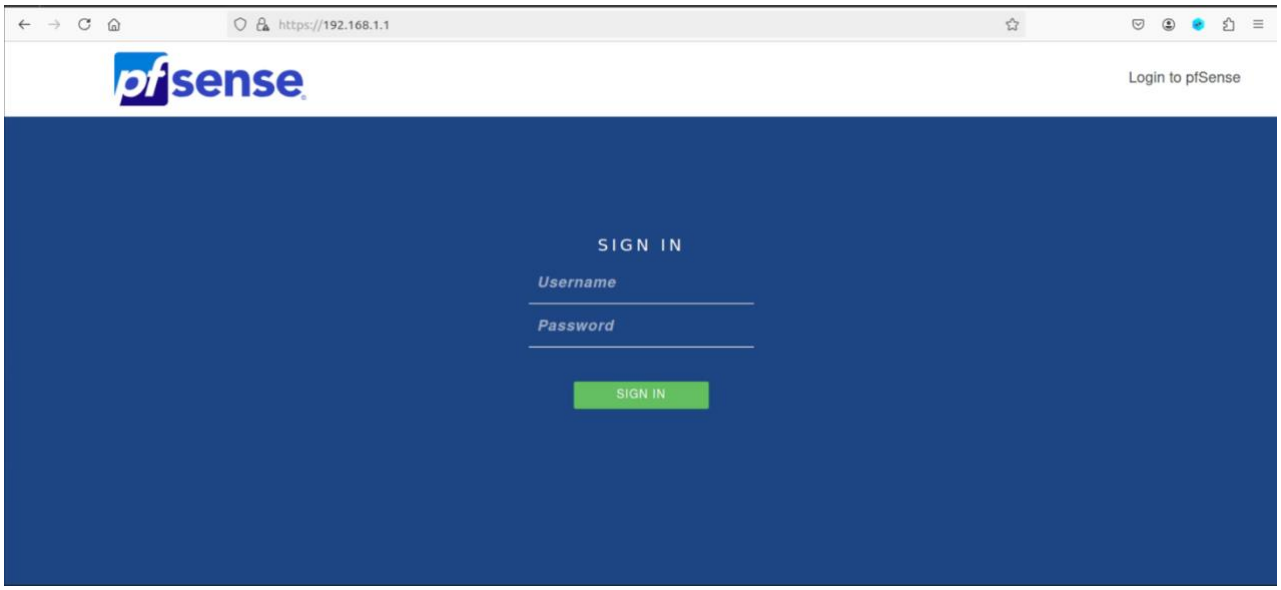
Lựa chọn cài đặt pfsense bản CE



Hình 6 Chọn Install CE

Tiếp tục các lựa chọn theo mặc định.

Sau khi cài đặt thành công, sử dụng máy A để truy cập vào pfsense thông qua địa chỉ http://192.168.1.1 với tài khoản và mật khẩu mặc định admin/pfsense.

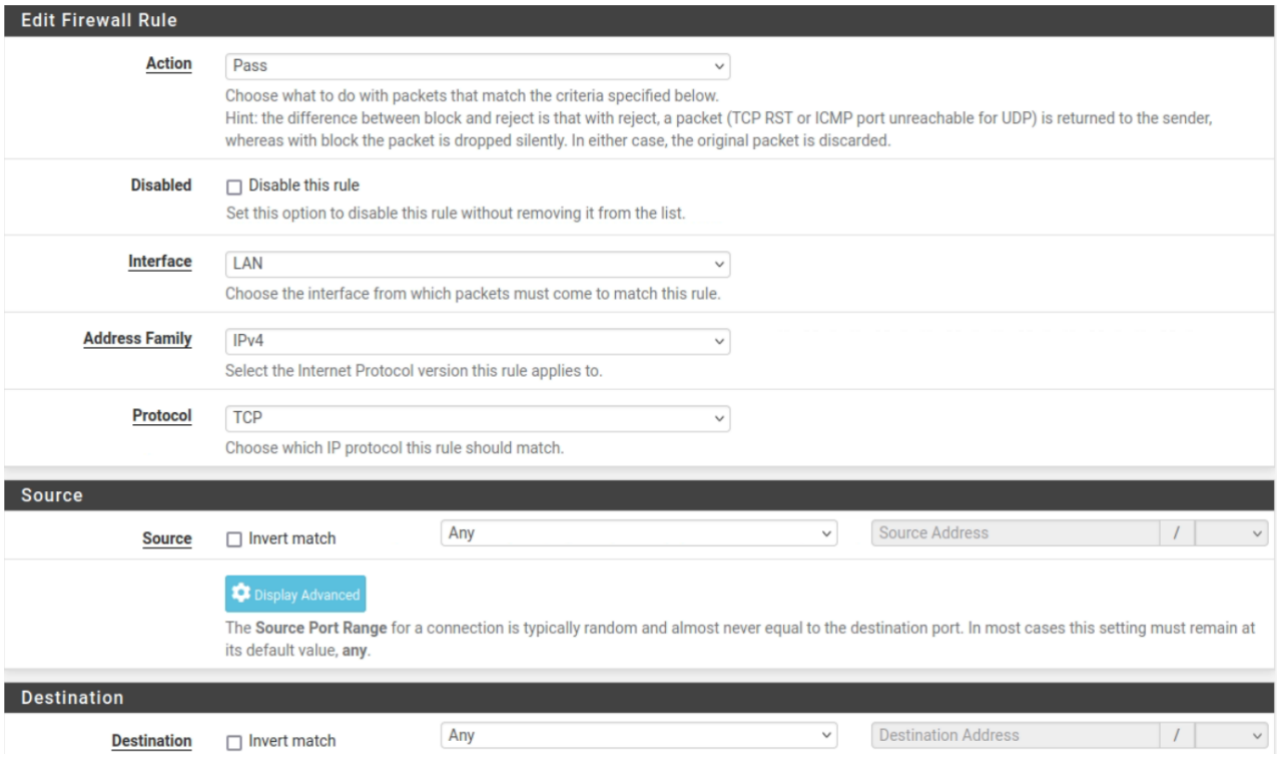


Hình 7 Màn hình đăng nhập pfsense

2. Thiết lập chính sách trên Firewall để bảo vệ mạng nội bộ

Có thể thực hiện cấu hình các luật của pfSense bằng cách vào Firewall → Rules→ Add. Trong đó:

- Action: Chọn Pass / Block / Reject tương ứng thao tác muốn thực hiện.
- Protocol: Các giao thức áp dụng cho luật này
- Source, destination: Các thông tin của gói tin để lọc (lớp mạng, địa chỉ host, cổng nguồn, cổng đích,…).



Hình 8 Cấu hình Rule pfsense

Task 1: Thiểu và thực hiện các rules sau (theo thứ tự):

1. Không cho phép các máy trong mạng nội bộ (192.168.1.0/24) thực hiện ping đến máy VM B.
2. Không cho phép các máy trong mạng nội bộ truy cập các website sử dụng giao thức http (cổng 80).
3. Chặn kết nối telnet từ mạng nội bộ ra bên ngoài.
4. Không cho phép các máy trong mạng nội bộ truy cập đến www.facebook.com và youtube.com.

Sau khi triển khai các rules trên, sử dụng máy VM A để kiểm tra.

3. Vượt qua sự kiểm soát của Firewall

Sau khi thực hiện các bước thiết lập các rules trong phần 2, lúc này máy VM A không thể nào thực hiện lênh telnet đến VM B, truy cập đến website www.facebook.com và các website sử dụng giao thức http. Mục tiêu của phần này là giúp máy A có thể vượt qua được sự giới hạn này nhưng không can thiệp đến các thiết lập của Firewall.

a. Thực hiện Telnet từ máy A đến máy B

Trên máy B, đảm bảo đã cài đặt gói telnetd và ssh (server). Từ máy A, khi thực hiện lệnh telnet đến máy B sẽ không kết nối được. Để vượt qua sự giới hạn này của Firewall, ta sẽ thiết

lập một SSH tunnel giữa máy A và máy B. Lúc đó, các traffic telnet sẽ được gửi và nhận thông qua tunnel này để vượt qua sự kiểm tra của firewall.
Từ máy A, sử dụng lệnh sau để thiết lập SSH tunnel:

```
$ ssh -fN -L 8000:localhost:23 VM_B_username@VM_B_IP

Ví dụ:

$ ssh -fN -L 8000:localhost:23 ubuntu@10.0.3.3
```

Sau khi thực hiện thiết lập tunnel trên, trên máy A thực hiện lệnh *telnet localhost 8000* để kết nối telnet đến máy B thông qua tunnel.

Task 2:

1. Trình bày ý nghĩa các tham số sử dụng trong 2 lệnh thiết lập tunnel và kết nối telnet ở trên.
2. Khi sử dụng lệnh telnet, thực chất các gói tin này có đi qua máy Firewall không? Nếu có, nguyên nhân tại sao Firewall không việc sử dụng telnet này? Nếu không, thì kết nối từ máy A đến máy B như thế nào để không đi qua máy Firewall?

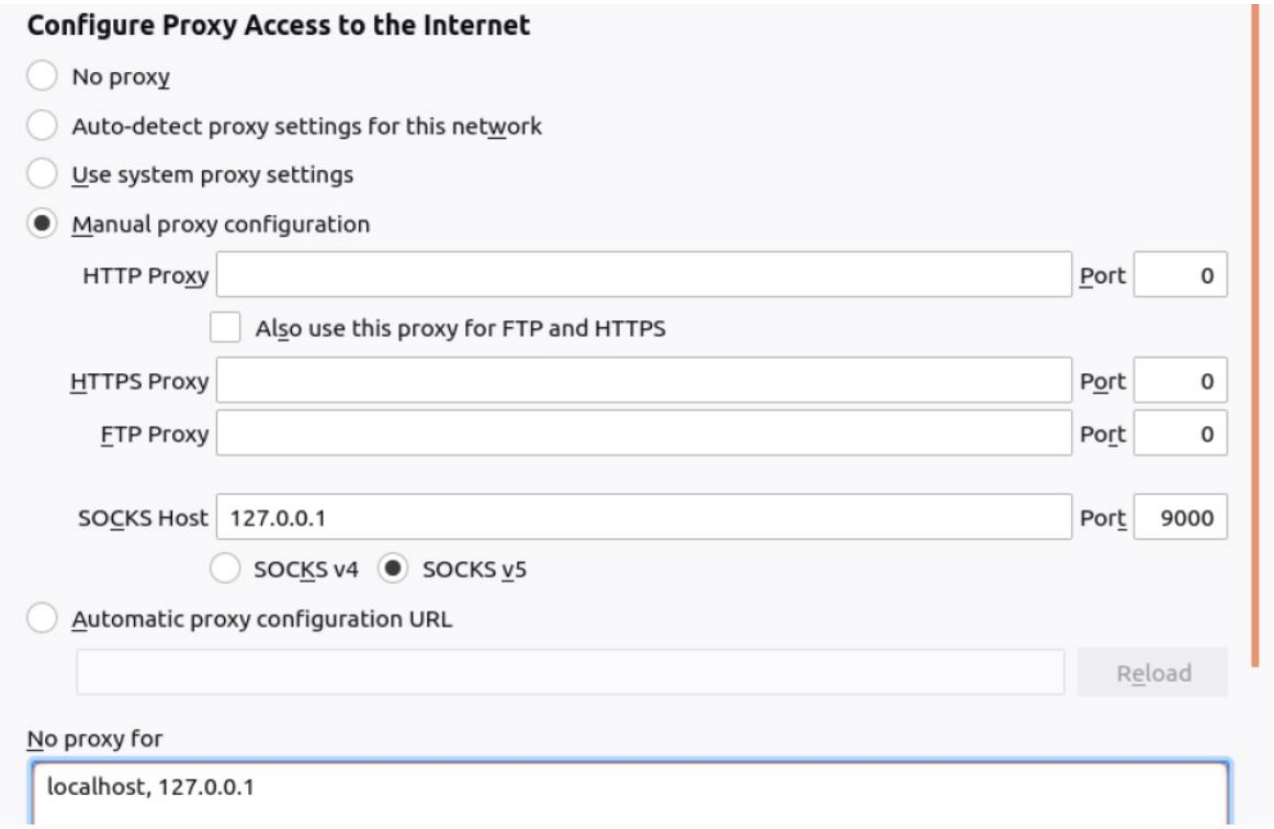
b. Kết nối đến Facebook sử dụng SSH Tunnel

Trong phần này, sẽ thực hiện tìm hiểu kỹ thuật dynamic port forwarding kết hợp với thiết lập sử dụng kết nối proxy trên trình duyệt. Trên máy VM A, thực hiện các thao tác sau:
Bước 1: Tạo SSH Tunnel

```
$ ssh -D 9000 -C VM_B_username@VM_B_IP
```

Bước 2: Cấu hình trình duyệt web (minh hoạt với trình duyệt Firefox) sử dụng kết nối proxy localhost:9000 để chuyển traffic sang tunnel vừa tạo khi truy cập internet. Từ Firefox browser, từ Menu → Preferences (hoặc gõ about:preferences vào thanh địa chỉ) → Network Settings → Chọn Settings.

- Chọn Manual proxy configuration
- Thiết lập SOCKS Host: 127.0.0.1 Port: 9000
- Chọn SOCKS_v5
- No Proxy for: localhost, 127.0.0.1



Hình 9 Thiết lập sử dụng Proxy để truy cập Internet cho trình duyệt

Bước 3: Sau khi thiết lập xong, thử truy cập website bất kỳ (google.com, youtube.com) xem có thể truy cập bình thường không? Nếu có, tunnel và proxy đã hoạt động tốt.

Task 3:

1. Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.
2. Thực hiện ngắt SSH Tunnel, xoá cache của trình duyệt và truy cập lại trang www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?
3. Nếu trên Firewall, áp dụng rule chặn kết nối SSH (port 22), lúc này có thể thiết lập tunnel này được hay không? Tại sao?

Bonus: Đề xuất giải pháp để phát hiện và ngăn chặn các cách thức vượt qua sự kiểm soát của Firewall trong trường hợp trên.

4. Triển khai Web Proxy (Application Firewall)

Trong các phần trên đã tìm hiểu về cách hoạt động của Filter Firewall thực hiện kiểm soát các gói tin ở tầng transport và thấp hơn. Trong phần này, sẽ tiến hành tìm hiểu về các thiết lập chính sách của Firewall ở tầng application bằng cách thiết lập web proxy và thực hiện một số yêu cầu trên web proxy này

a. Cài đặt và cấu hình Squid

Cài đặt web proxy server trên máy ảo VM B

```
# apt-get install squid

# service squid start //khởi động service

# service squid restart //Khởi động lại service
```

Trên máy VM A, cấu hình trình duyệt để sử dụng kết nối proxy qua proxy server của VM B. Từ Firefox browser, truy cập vào phần thiết lập Network.

```
Chọn Manual proxy configuration

HTTP Proxy: Địa chỉ IP của máy VM B Port: 3128

HTTP Proxy: Địa chỉ IP của máy VM B Port: 3128
```

Mặc định, squid sẽ chặn truy cập tất cả các trang web. Để cho phép truy cập, điều chỉnh trong file /etc/squid/squid.conf và khởi động lại squid.

```
Tìm

http_access deny all

Thay thành

http_access allow all
```

Từ máy A, truy cập vào các trang web https://google.com để kiểm tra web proxy đã hoạt động hay chưa. Máy A có thể truy cập được website https://www.facebook.com không? Nếu có, giải thích tại sao Firewall đã chặn máy A truy cập mà vẫn có thể truy cập được. Nếu không, giải thích lý do tại sao? Mô tả cơ chế hoạt động.

b. Thiết lập chuyển hướng (Rewrite / URL Redirection)

Tại máy B, tạo file script sau (/etc/squid/script.pl) sử dụng ngôn ngữ Perl và cấp quyền (chmod) cho phép thực thi (chmod +x /etc/squid/script.pl)

```
 #!/usr/bin/perl -w
use strict;
use warnings;
# Forces a flush after every write or print on the STDOUT
select STDOUT; $| = 1;
# Get the input line by line from the standard input.
# Each line contains an URL and some other information.
while (<>)
{
my @parts = split;
my $url = $parts[0];
if ($url =~ /example\.com/)
{
```

```
# URL Rewriting
print "http://www.uit.edu.vn\n";
}
else
{
# No Rewriting.
print "\n";
}
```

Tìm trong file cấu hình /etc/squid/squid.conf và chỉnh sửa thành nội dung dưới đây để sử dụng url_rewrite_program với chương trình trên. Sau đó, khởi động lại squid.

```
url_rewrite_program /etc/squid/script.pl

url_rewrite_children 5
```

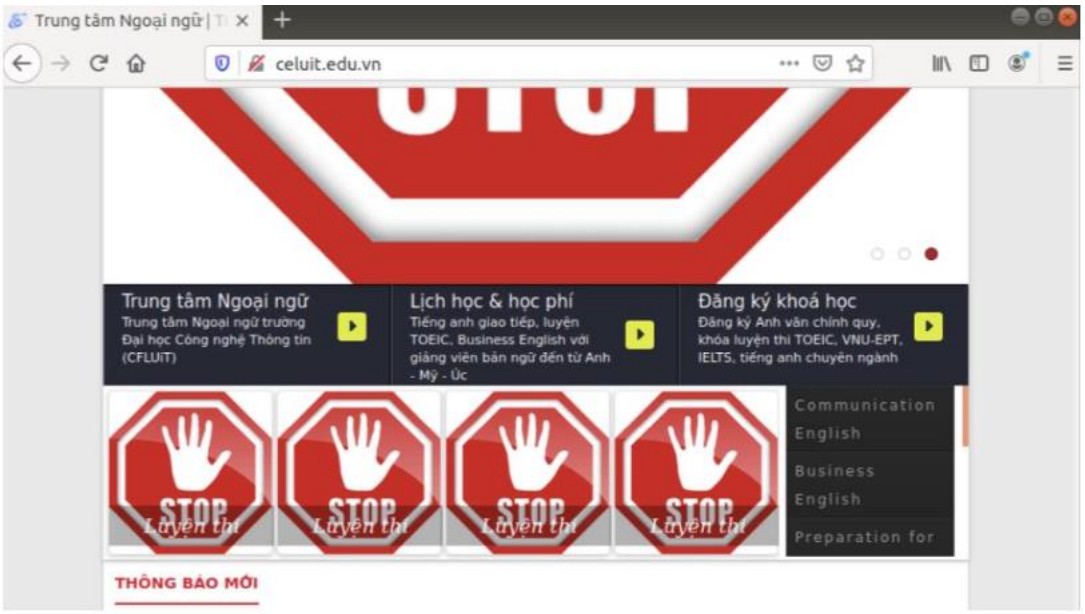
Từ máy A, sử dụng trình duyệt truy cập vào website http://example.com ta thấy tự động chuyển sang website http://www.uit.edu.vn thì đã cấu hình đúng.

Lưu ý: Bản cài đặt mặc định của Squid chưa thể xử lý các trang web sử dụng giao thức https. Cần phải biên dịch lại từ mã nguồn của Squid với các tuỳ chọn bổ trợ phù hợp cho giao thức https thì mới có thể xử lý được.

Task 4:

1. Đoạn chương trình script.pl trên hoạt động như thế nào?
2. Thay đổi nội dung đoạn chương trình trên để khi truy cập vào website example.com, một hình ảnh cảnh báo dừng lại xuất hiện (như hình dưới).
3. Thay đổi nội dung chương trình để khi truy cập website, tất cả các hình ảnh đều được thay bằng hình ảnh bạn thích (như hình minh hoạ dưới).

Hình 10 Minh hoạ xuất hiện cảnh báo dừng lại khi truy cập example.com



Hình 11 Minh hoạ thay thế các ảnh trong website bằng squid

5. VPN

Một trong những chức năng chính của VPN là tạo kết nối an toàn cho phép kết nối từ xa đến mạng nội bộ. Tính năng VPN cũng được tích hợp sẵn trên Firewall pfSense.

Để tăng cường bảo mật, mặc định pfSense sẽ bật tính năng "Block private networks and loopback addresses". Nên không thể thực hiện các thao tác như ping đến WAN Interface được. Sinh viên cần bỏ chọn tuỳ chọn này (Interface → WAN) nếu muốn thực hiện ping,… đến WAN Interface.

Task 5:

1. Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức này có đặc điểm gì khác nhau?
2. Tìm hiểu và thực hiện cấu hình trên pfSense, sao cho từ máy VM B có thể mở kết nối VPN đến pfSense server để truy cập được máy VM A.

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.
- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.

- Ví dụ: [NT140.P12.ANTT.1]-Lab1_2252xxxx_2252yyyy.
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!