

4

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Khai thác tường lửa trong Linux

Linux Firewall Exploration

Thực hành môn An toàn Mạng máy tính



Tháng 10/2021

Lưu hành nội bộ

<Ng nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

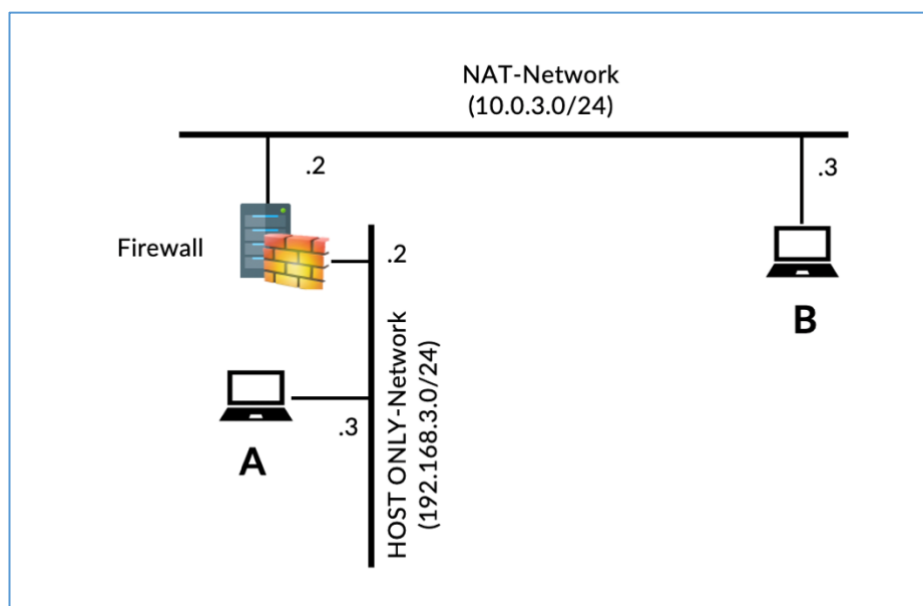
- Tìm hiểu về cách thức hoạt động của tường lửa và thực hiện triển khai tường lửa đơn giản.
- Tìm hiểu về Virtual Private Network (VPN) và cách thức thiết lập kết nối VPN. Sử dụng VPN để vượt qua sự kiểm soát của tường lửa.

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 07 ngày.

3. Môi trường thực hành

Trong bài thực hành này, sinh viên cần chuẩn bị 03 máy ảo như trong mô hình bên dưới.



Hình 1. Mô hình mạng sử dụng trong bài thực hành

Trong đó:

- Firewall VM: Được cài đặt pfSense để bảo vệ lớp mạng 192.168.3.0/24.
- VM B sẽ đóng vai trò trung gian giúp VM A có thể truy cập các website và dịch vụ mạng bên ngoài bị chặn bởi firewall.

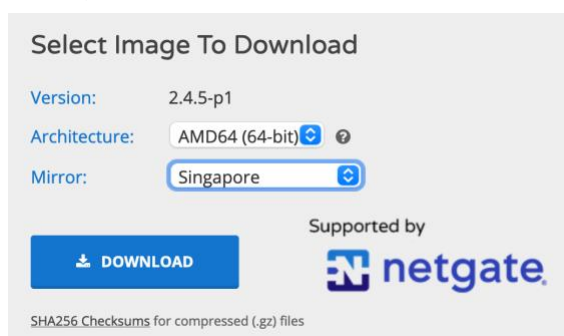
Máy ảo	Interfaces	Thông tin
Firewall	NAT 10.0.3.2/24	Cài đặt pfSense (hướng dẫn trong phần 1 – Nội dung thực hành) sử dụng 2 card mạng: <ul style="list-style-type: none"> Card NAT: dùng để kết nối ra internet; Card Host Only: để kết nối đến VM A
	Host Only 192.168.3.2/24	
VM A	Host Only 192.168.3.3/24 Gateway: 192.168.3.2	Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng Host Only để kết nối đến máy Firewall.
VM B	NAT 10.0.3.3/24	Hệ điều hành Ubuntu (khuyến khích phiên bản 18.04 trở lên) sử dụng card mạng NAT để kết nối đến Internet. Cài đặt thêm telnetd và ssh (server).

B. THỰC HÀNH

Lưu ý: Sinh viên lần lượt thực hiện theo thứ tự từng phần, theo các bước hướng dẫn trong bài lab.

1. Cài đặt pfSense firewall

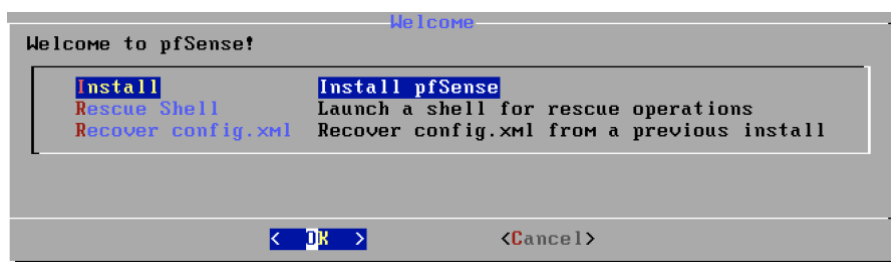
Sinh viên tải về file cài đặt pfsense với bản cài CD Image (iso) Installer từ trang web <https://www.pfsense.org/download/>. Sau khi tải về, tiến hành giải nén (.gz) để được file .iso và thực hiện cài đặt máy ảo.



Hình 2. Tải xuống bản cài đặt pfSense

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)
- **Bước 1:** Khởi động máy ảo từ đĩa CD (file iso cài đặt) cài pfSense
- **Bước 2:** Chọn cài đặt “Install pfSense”



Hình 3. Cài đặt pfSense

- **Bước 3:** Thực hiện các bước theo hướng dẫn của trình cài đặt. Quá trình cài đặt sẽ yêu cầu khởi động lại để đến bước cấu hình.
- **Bước 4:** Sau khi khởi động lại, sẽ thấy xuất hiện thông tin 2 card mạng để tiến hành cấu hình. Sinh viên cần xác định card mạng nào là NAT, card mạng nào là Host Only (dựa vào MAC address).

```
le0      00:0c:29:47:dd:c8 (down) AMD PCnet-PCI
le1      00:0c:29:47:dd:d2 (down) AMD PCnet-PCI
```

- **Bước 5:** Có thể bỏ qua phần thiết lập VLAN (không sử dụng trong nội dung bài lab này). Chọn No

```
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y:n]? No
```

- **Bước 6:** 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. Sinh viên lưu ý chọn đúng card mạng cho các interface và xác nhận để tiếp tục cài đặt.

```
Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le0
```

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished): le1
```

```
The interfaces will be assigned as follows:
WAN  -> le0
LAN  -> le1
```

- **Bước 7:** Thực hiện đặt lại địa chỉ ip cho các interfaces:

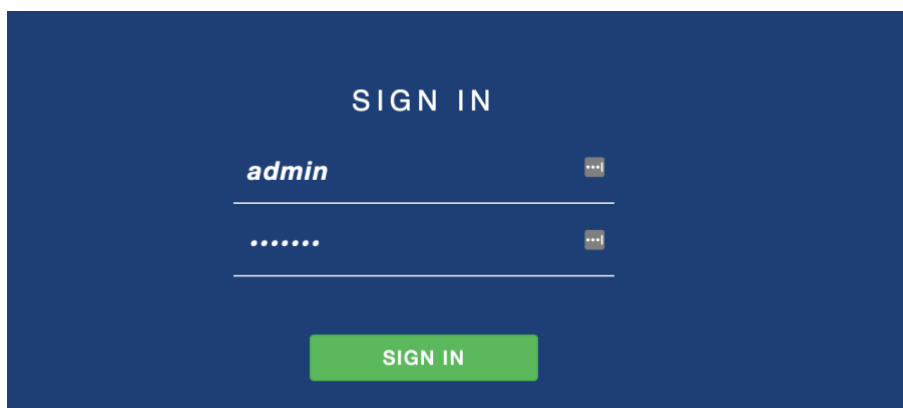
```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

```

Chọn mục số 2 → Chọn Interface cần cấu hình:

- Đối với WAN interface: tắt DHCP, đặt địa chỉ IP: 10.0.3.2, subnet mask: 24; WAN IPv4 upstream gateway address: địa chỉ gateway của mạng NAT (10.0.3.1); không sử dụng IPv6.
 - Đối với LAN interface: Đặt địa chỉ IP: 192.168.3.2, subnet mask: 24.
- **Bước 8:** Truy cập trang quản trị: Trên máy thật, mở trình duyệt web và truy cập đến địa chỉ <http://192.168.3.2>



Lưu ý: Có thể thực hiện các thông số cấu hình ở trên thông qua giao diện web.

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,...).

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

any

Destination Address

/

Destination Port Range

(other)

From

Custom

To

(other)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Sinh viên tìm hiểu và thực hiện các rules sau (theo thứ tự):

1. Không cho phép các máy trong mạng nội bộ (192.168.3.0/24) 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

Sinh viên cần hoàn thành nội dung trong phần 2 trước khi thực hiện phần này. Sau khi thực hiện các bước thiết lập các rules trong phần 2, lúc này máy VM A không thể nào thực hiện lệnh 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.

```
ubuntu@ubuntu:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 18.04.5 LTS
ubuntu login: ubuntu
Password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-52-generic x86_64)
```

® Bài tập về nhà (yêu cầu làm)

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
```

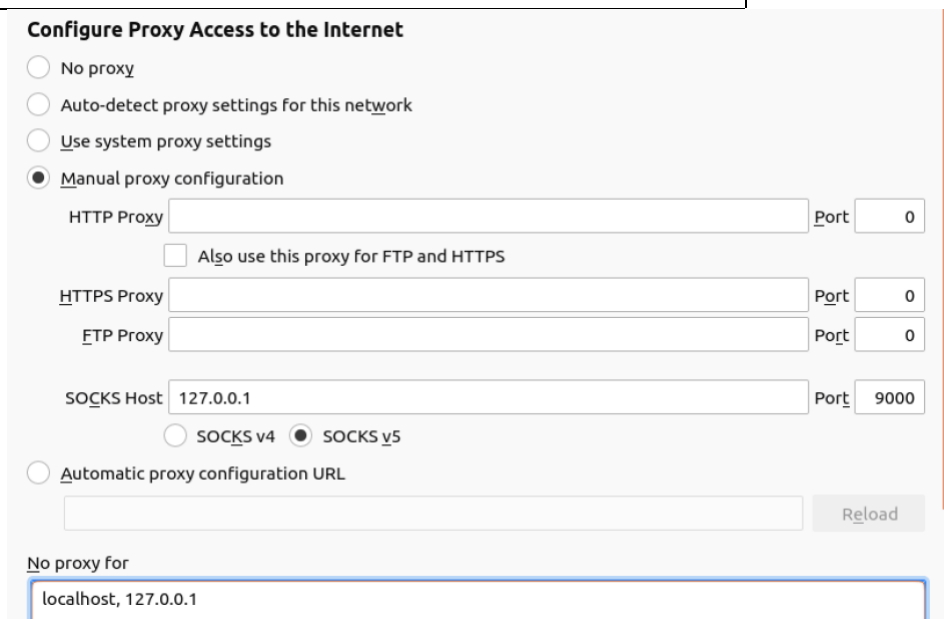
- **Bước 2:** Cấu hình trình duyệt web (minh hoạt với trình duyệt Firefox) sử dụng kết nối proxy localhost:9000 để chuyển traffic sang tunnel vừa tạo khi truy cập internet. Từ Firefox browser, từ Menu → Preferences (hoặc gõ about:preferences vào thanh địa chỉ) → Network Settings → Chọn Settings

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



The screenshot shows the 'Configure Proxy Access to the Internet' dialog box in Firefox. The 'Manual proxy configuration' option is selected. The 'SOCKS Host' is set to '127.0.0.1' and the 'Port' is '9000'. The 'SOCKS v5' radio button is selected. The 'No proxy for' field contains 'localhost, 127.0.0.1'.

Hình 4. 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.

® Bài tập (yêu cầu làm)

3. Truy cập website www.facebook.com. Mô tả quá trình bạn quan sát được.
4. Thực hiện ngắt SSH Tunnel, xóa cache của trình duyệt và truy cập lại trang www.facebook.com. Lúc này, còn truy cập được trang web Facebook không?
5. 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?

® Bài tập mở rộng (cộng điểm)

6. 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

- **Bước 1:** 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
```

- **Bước 2:** 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
```

- **Bước 3:** 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
```

- **Bước 4:** 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.

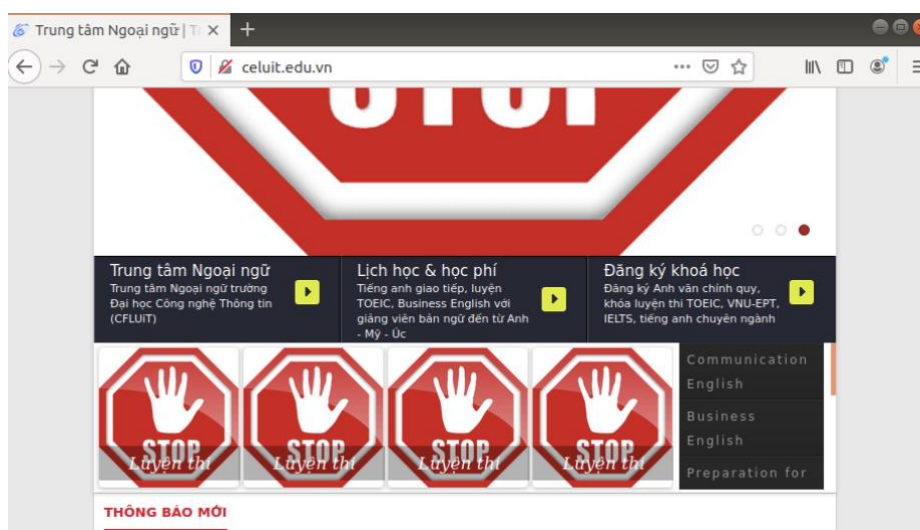
Lưu ý: Bản cài đặt mặc định của Squid chưa thể xử lý các trang web sử dụng giao thức https. Cần phải biên dịch lại từ mã nguồn của Squid với các tùy chọn hỗ trợ phù hợp cho giao thức https thì mới có thể xử lý được.

[®] Bài tập (yêu cầu làm)

7. Đoạn chương trình `script.pl` trên hoạt động như thế nào?
8. 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).
9. 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 họa dưới).



Hình 5. Minh họa xuất hiện cảnh báo dừng lại khi truy cập example.com



Hình 6. Minh họa 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 tùy chọn này (Interface → WAN) nếu muốn thực hiện ping,... đến WAN Interface.

Block private networks and loopback addresses

☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Bài tập về nhà (yêu cầu làm)

10. Firewall pfSense hỗ trợ các giao thức thiết lập kết nối VPN nào? Những giao thức này có đặc điểm gì khác nhau?

11. 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.

6. Lưu ý khi nộp bài

Trước khi nộp bài, sinh viên thực hiện thao tác sao lưu cấu hình trên pfSense và nộp kèm theo báo cáo.

- **Bước 1:** Trên giao diện web quản lý pfSense. Chọn Diagnostics → Backup & Restore.
- **Bước 2:** Trong phần Backup Configuration, chọn như hình sau. Sau đó chọn “Download configuration as XML”

Backup Configuration	
Backup area	All
Skip packages	<input type="checkbox"/> Do not backup package information.
Skip RRD data	<input checked="" type="checkbox"/> Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)
Encryption	<input type="checkbox"/> Encrypt this configuration file.
Download configuration as XML	

- **Bước 3:** Kèm theo file vừa XML vừa download khi nộp báo cáo.

C. YÊU CẦU & ĐÁNH GIÁ**1. Yêu cầu**

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (tối đa 2 sinh viên/nhóm). Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài bằng **1 trong 2 hình thức**:

a) Báo cáo chi tiết:

Báo cáo cụ thể quá trình thực hành (có ảnh minh họa các bước) và giải thích các vấn đề kèm theo. Trình bày trong file PDF theo mẫu có sẵn tại website môn học và source-code của chương trình.

b) Video trình bày chi tiết:

Quay lại quá trình thực hiện Lab của sinh viên kèm thuyết minh trực tiếp mô tả và giải thích quá trình thực hành. Upload lên **Youtube** và chèn link vào đầu báo cáo theo mẫu. **Lưu ý:** Không chia sẻ ở chế độ Public trên Youtube.

Đặt tên file báo cáo theo định dạng như mẫu:

[Mã lớp]-LabX_GroupY

Ví dụ: [NT101.I11.1]-Lab1_Group2.

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện và chứng minh được do nhóm sinh viên thực hiện.
- Hoàn tất nội dung cơ bản và có thực hiện nội dung *mở rộng – cộng điểm* (với lớp ANTN).

Kết quả thực hành cũng được đánh giá bằng kiểm tra kết quả trực tiếp tại lớp vào cuối buổi thực hành hoặc vào buổi thực hành thứ 2.

Lưu ý: Bài sao chép, nộp trễ, “*gánh team*”, ... sẽ được xử lý tùy mức độ.

Nội dung bài thực hành được biên soạn dựa trên bộ thực hành “Network Security Lab” của SEED LABS.

HẾT

Chúc các bạn hoàn thành tốt!