LAB 04 – INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Môi trường thực hành:

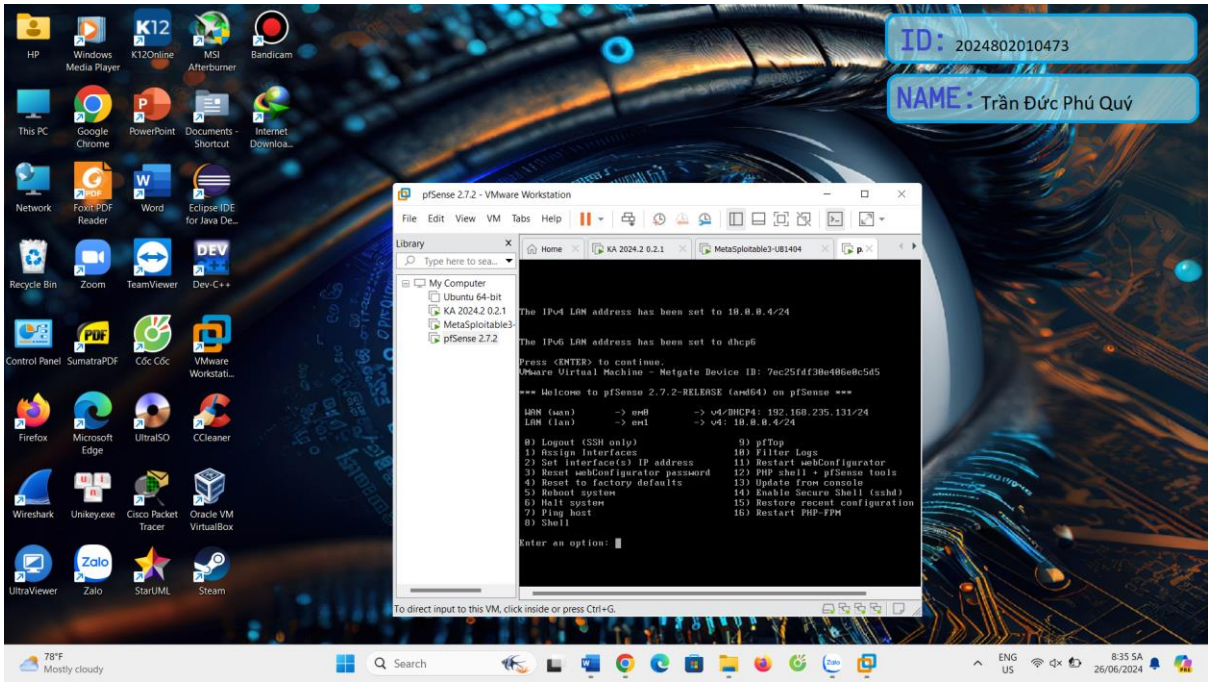
3 Máy ảo (VM): Controller, Server, Attacker

Các công cụ: Suricata

1. Basic pfSense (3Đ)

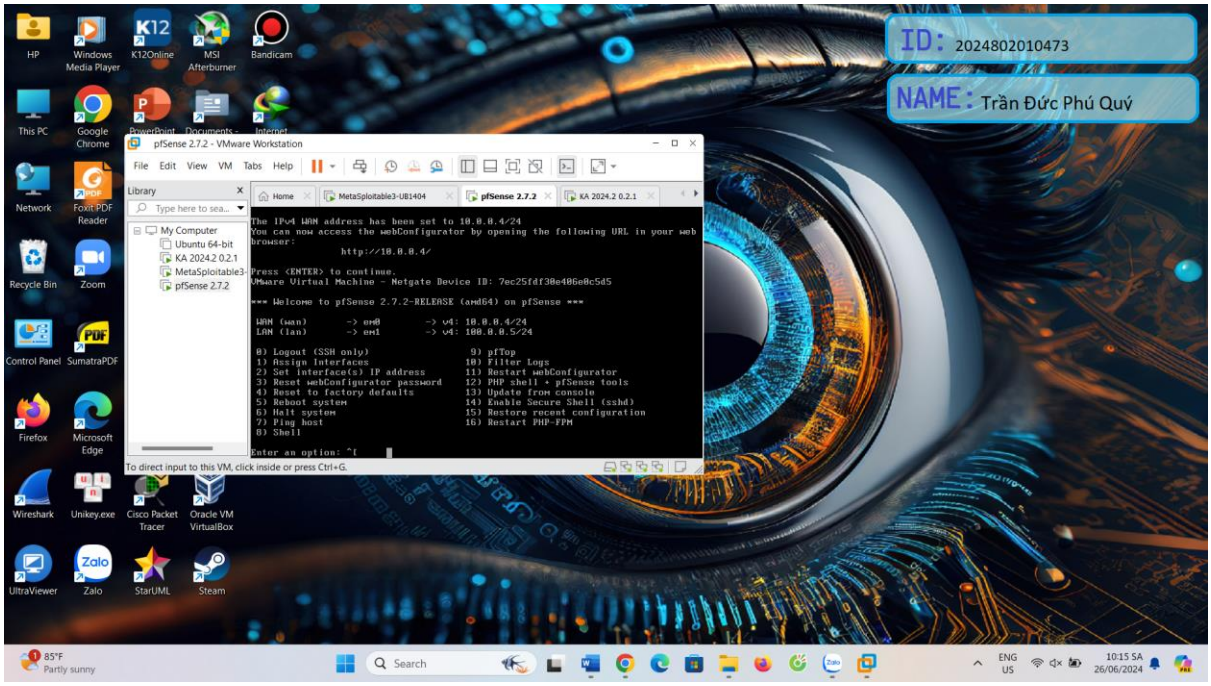
Trên **Controller**, Đăng nhập với quyền admin

1.1. Thiết lập IP 10.0.0.4/24 cho ethernet đang gắn vào VMnet 2



Gợi ý: Tùy chọn 2) từ menu chính

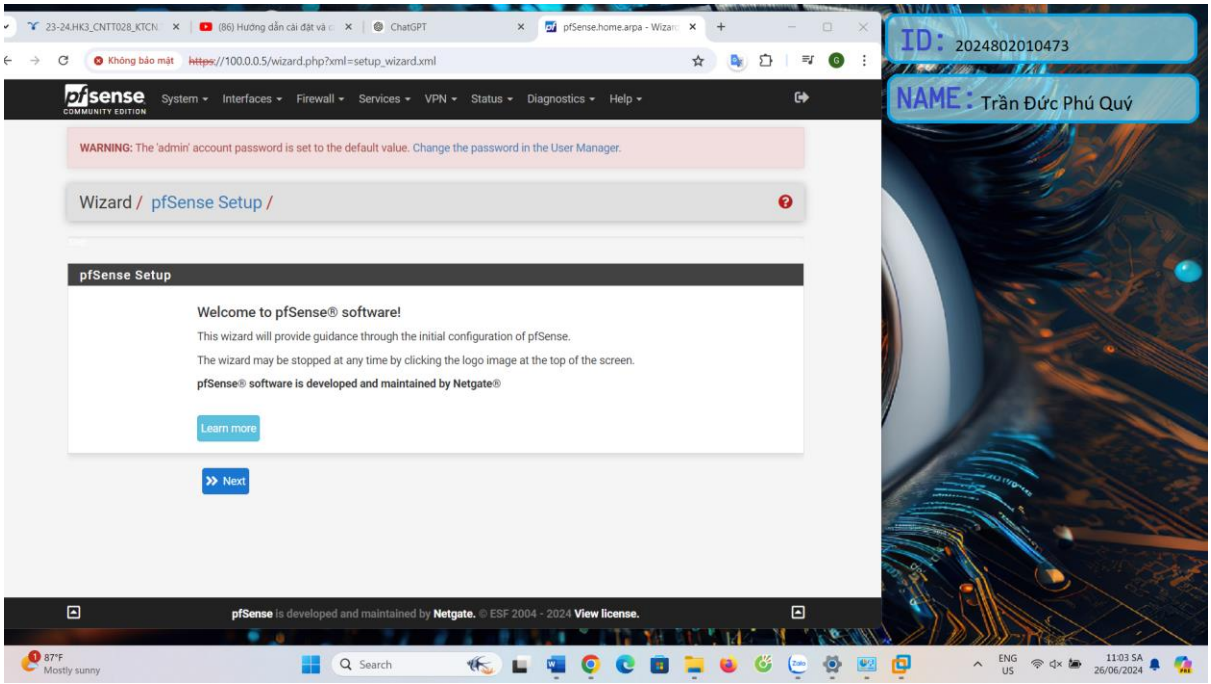
1.2. Thiết lập IP 100.0.0.5/24 cho ethernet đang gắn vào VMnet 3



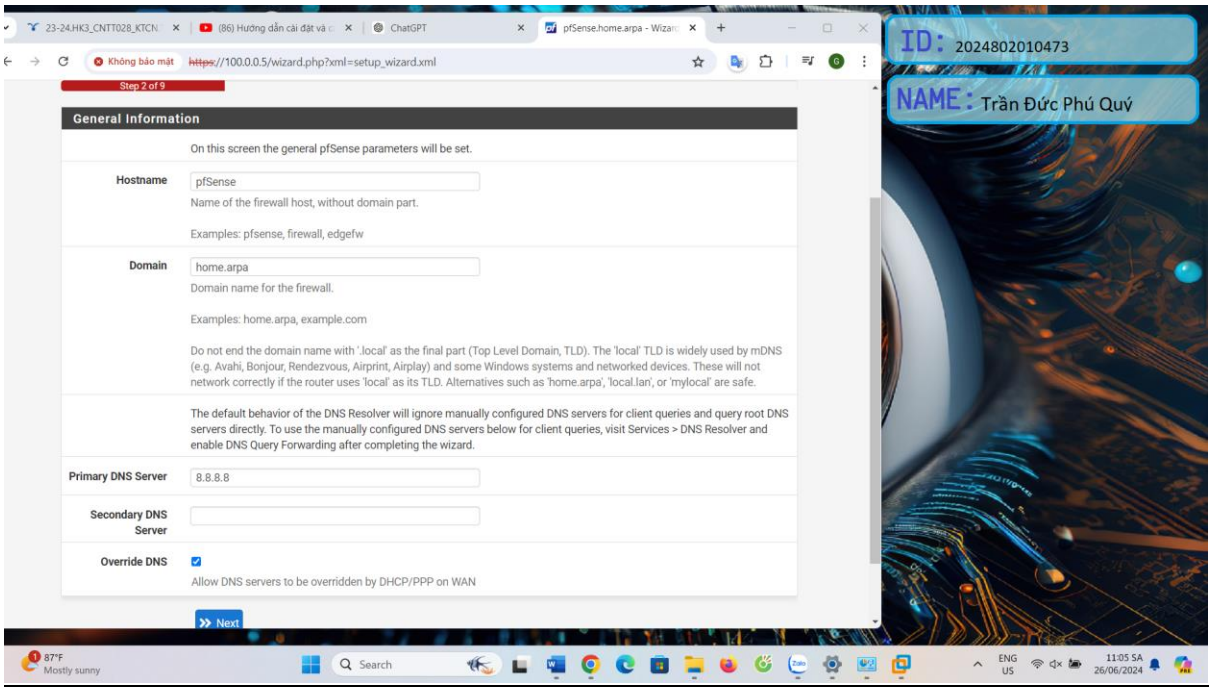
Gợi ý: Tùy chọn 2) từ menu chính

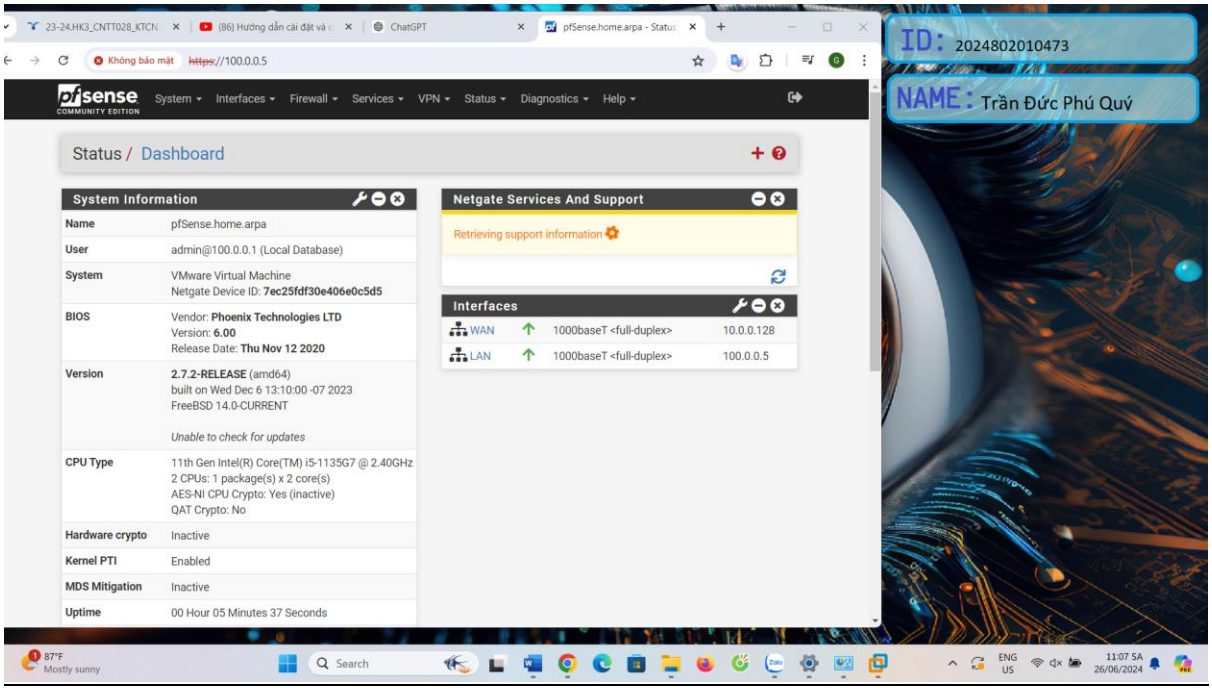
1.3. Truy cập giao diện pfSense từ **máy thật** thông qua IP LAN của Vmnet 3 hoặc VMnet 2

Gợi ý: Sử dụng tính năng “Edit” -> “ Virtual Network Editor” để tạo VMnet 2 và VMnet 3 nếu chưa có, thiết lập IP của vmnet2 là 10.0.0.2/24 và vmnet3 là 100.0.0.3/24 (Vô hiệu hóa chức năng DHCP server)



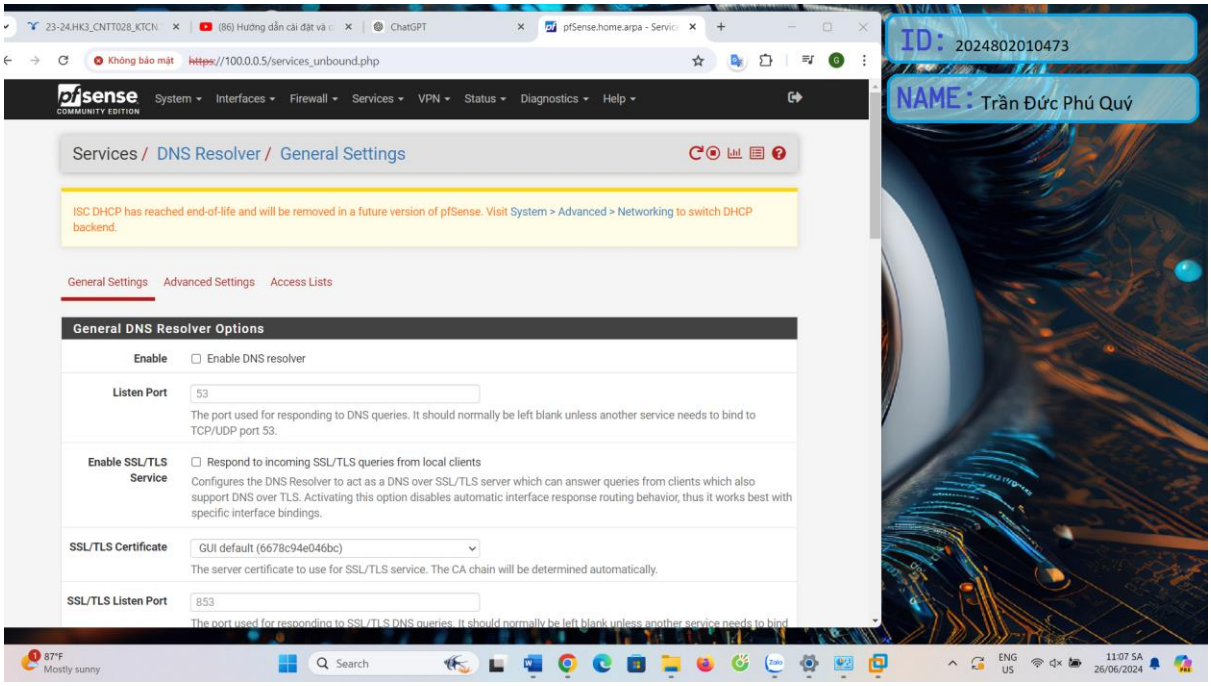
1.3. Thiết lập thông tin ban đầu cho pfSense:





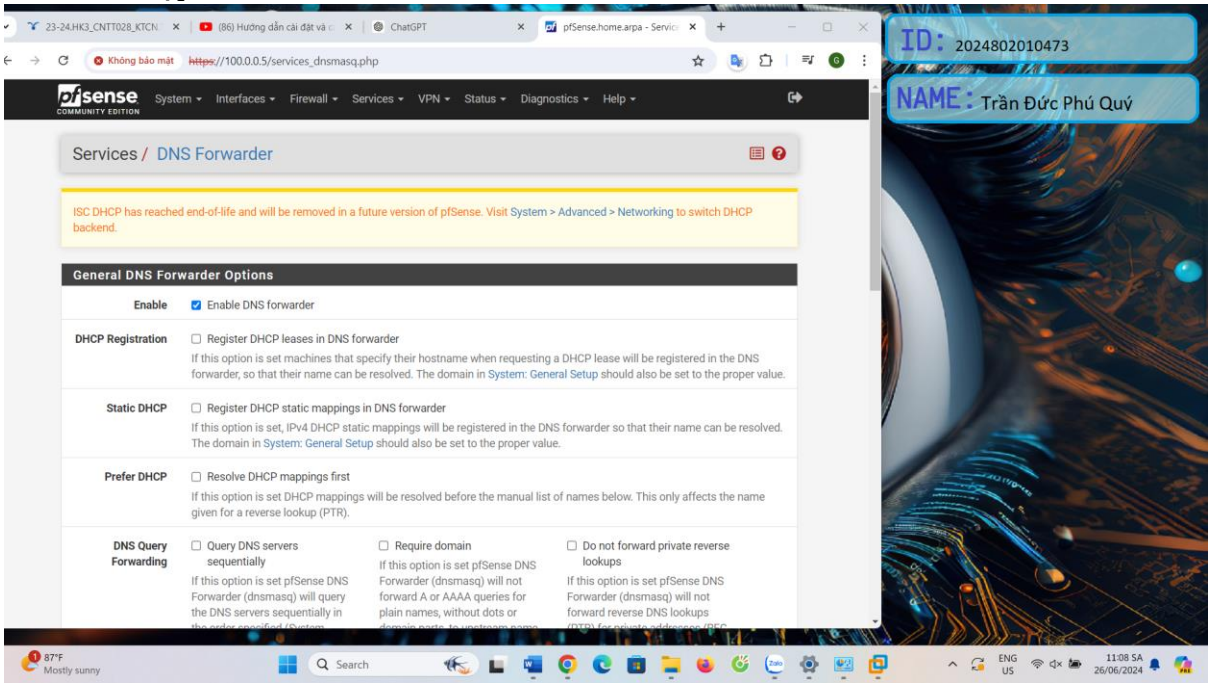
Gợi ý: thiết lập tùy ý, primary DNS Server: 8.8.8.8 ; phần thiết lập WAN bỏ chọn mục “RFC1918 Networks” và “Block bogon networks”

1.4. Tắt DNS resolve



Gợi ý: Menu [Services]

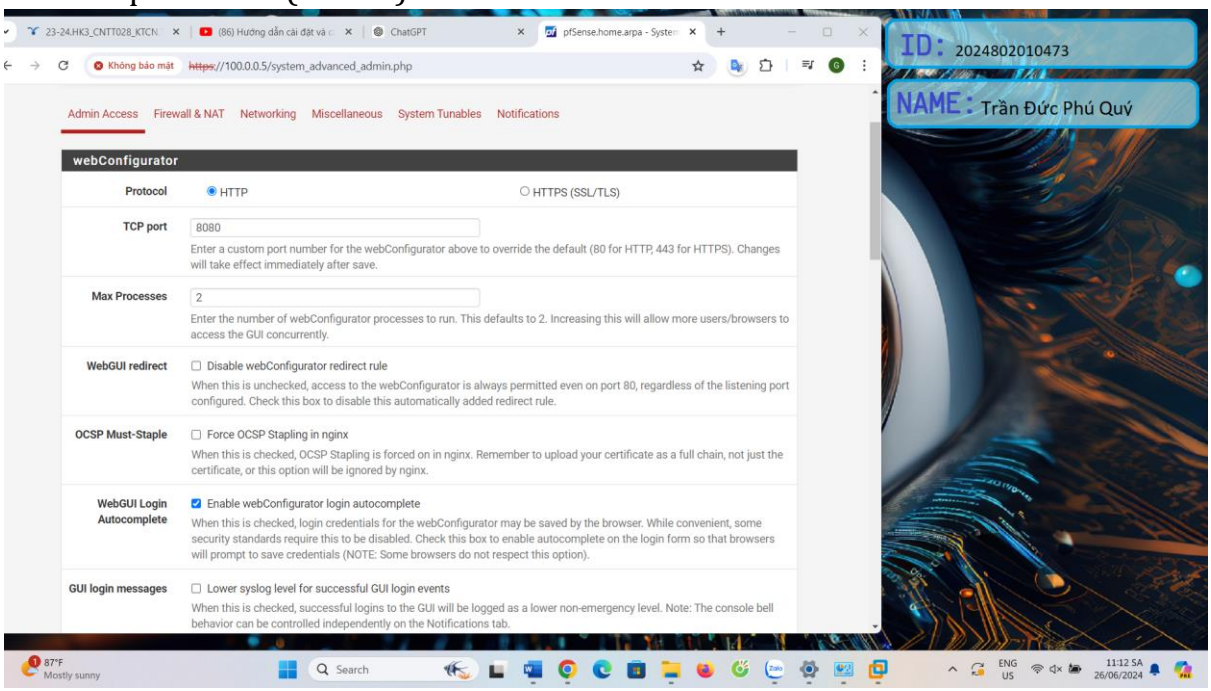
1.5. Thiết lập DNS forwarder:



Gợi ý: Menu [Services]

1.5. Thiết lập Port forward

Cấu hình để truy cập IP 100.0.0.5 port 80 của pfsense sẽ chuyển hướng đến IP 10.0.0.8 port 8080 (Server)

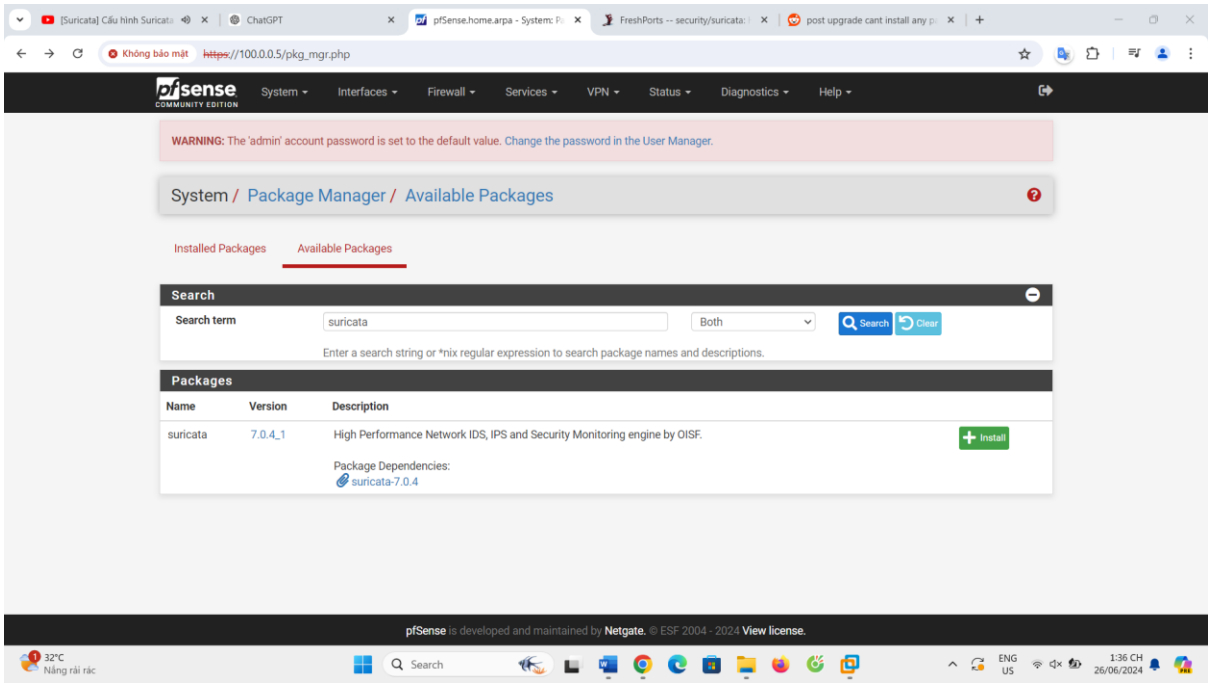


Gợi ý: Menu [System] [Advanced] để đổi port 80 của controller thành port khác

Menu [Firewall] [NAT] -> Add … để cấu hình NAT Port

2. Suricata (4Đ)

2.1. Cài đặt Suricata



Gợi ý: Menu [System] [Package Manager] ...

2.2. Thiết lập Suricata

Replace me

Gợi ý: menu [Service] [Suricata]

2.3. Thiết lập giám sát trên interface gắn với VMnet 3

Replace me

Gợi ý: tắt offloading trong Network Interface , khi lưu cấu hình sẽ khởi động lại .

2.4. Cập nhật Các rule có sẵn

Replace me

Gợi ý: Check option ETOpen, Snort GPLv2 -> Updates > Forces .

2.5. Thiết lập rule có sẵn

Replace me

Gợi ý: [interface] -> Select All -> save

3. Basic Attacker, Server and Controller Respond(3Đ)

Trên **Server**, Đăng nhập với quyền root

3.1. Thiết lập IP tĩnh 10.0.0.6/24 cho ethernet đang gắn vào vmnet 2

Replace me

Trên **Attacker**, Đăng nhập với quyền root, thiết lập IP tĩnh 100.0.0.7/24 đang gắn vào vmnet3

3.2. **Attacker** Thử quét port **Controller** bằng NMAP

Replace me

3.3. Chuyển sang web của **Controller** , Kiểm tra các cảnh báo

Replace me

3.4. Attacker Thử quét site **Controller** bằng Nikto

Replace me

3.5. Chuyển sang web của **Controller** , Kiểm tra các cảnh báo trong Alert

Replace me

3.6.Trên **Controller**, thử chọn [interface] và bật "Block offenders"

Replace me

3.7. Trên **Attacker** thử quét lại bằng Nmap, nikto, truy cập lại web

Replace me