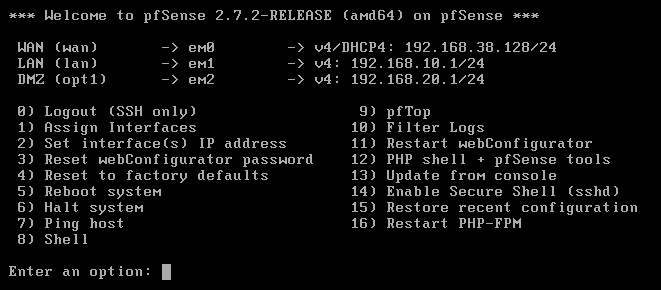
# **CHƯƠNG 3: TRIỂN KHAI TƯỞNG LỬA BẰNG PFSENSE**

## 3.1. Chuẩn bị

* 01 máy ảo hệ điều hành Windows 10:
* Sử dụng card mạng VmNet2 (Host-only).
* Địa chỉ IP: 192.168.10.150
* Default gateway: 192.168.10.1
* 01 máy ảo hệ điều hành Ubuntu (đã cài Webserver DVWA):
* Sử dụng card mạng VmNet3 (Host-only).
* Địa chỉ IP: 192.168.20.100
* Default gateway: 192.168.20.1
* 01 máy ảo hệ điều hành Windows server 2012
* Sử dụng card mạng VmNet2 (Host-only).
* Địa chỉ IP: 192.168.10.100
* Default gateway: 192.168.10.1
* 01 máy ảo hệ điều hành Kali Linux:
* Sử dụng card mạng NAT
* Địa chỉ IP: 192.168.38.130
* Default gateway: 192.168.38.128
* 01 máy ảo Pfsense làm tường lửa:



## 3.2. Mô hình

A diagram of a computer server

Description automatically generated

* WAN: 192.168.38.0/24. Sử dụng card mạng NAT – Phân vùng mạng kết nối Internet.
* LAN: 192.168.10.0/24. Sử dụng card mạng VmNet2 (Host-only) – Phân vùng mạng nội bộ.
* DMZ: 192.168.20.0/24. Sử dụng card mạng VmNet3 (Host-only) – Phân vùng đặt các máy chủ Web.

## 3.3. Cấu hình tường lửa cơ bản

- Cấu hình IP tĩnh (Static IP Address)

Chọn số 2: Set interface(s) IP address

A screen shot of a computer

Description automatically generated

Chọn tiếp số 2: Chọn LAN

A screenshot of a computer screen

Description automatically generated

* Hỏi về DHCP thì chọn n
* Nhập IP: 192.168.10.1 và Subnet: 24
* Bỏ qua các bước còn lại

- Sử dụng trình duyệt trên máy Win 10 để quản trị tưởng lửa PfSense qua giao diện.

Truy cập theo đường dẫn: <http://192.168.10.1>

A screenshot of a login screen

Description automatically generated

* Username: admin
* Password: pfsense

## 3.4. Thiết lập luật theo kịch bản

### **3.4.1. Thiết lập luật trong mạng LAN**

**a. Chặn toàn bộ máy trong mạng LAN không truy cập được mạng**

Mặc định pfSense cho phép các clinet trong mạng LAN có thể truy cập mạngA screenshot of a computer

Description automatically generated

* Đây là các rule mặc định

Ta bấm vào hình bút chì để chỉnh sửa rule và chọn disabled để vô hiệu hoá rule.

A screenshot of a computer

Description automatically generated

Kết quả cả 2 máy trong mạng LAN không truy cập được internet

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**b. Chỉ cho phép 1 máy trong mạng LAN được truy cập vào phần cài đặt (web GUI) của tường lửa pfSense.**

Ở đây, ta sẽ tiến hành cho phép chỉ máy Windows 10 được truy cập vào phần cài đặt (web GUI) của tường lửa pfSense.

Ta bấm Add để tạo rule mới trong Firewall/ Rules/ LAN

A screenshot of a computer

Description automatically generated

* **Thêm rule cho phép địa chỉ máy Windows 10 truy cập**
* **Action**: Pass
* **Interface**: LAN
* **Address Family**: IPv4
* **Protocol**: TCP
* **Source**: Address or alias → nhập IP: 192.168.10.150
* **Destination**: This Firewall
* **Destination port range**: HTTPS (443)

A screenshot of a computer

Description automatically generated

* **Thêm rule chặn tất cả các địa chỉ IP khác truy cập**
* **Action**: Block
* **Interface**: LAN
* **Address Family**: IPv4
* **Protocol**: TCP
* **Source**: any
* **Destination**: This Firewall
* **Destination port range**: HTTP (80)

Kết quả máy Windows server 2012 không thể truy cập vào trang cài đặt tường lửa

A screenshot of a computer

Description automatically generated

**c. Chặn web với Aliase**

Ta sẽ chặn 2 trang web Facebook, Youtube.

A screen shot of a computer code

Description automatically generated

A screen shot of a computer screen

Description automatically generated

Sau đó ta vào Firewall/Aliases/IP

Chọn Add để tạo nhóm các IP, ở đây có tên Blockweb

A screenshot of a computer

Description automatically generated

* Cấu hình như hình trên

Tiếp đến ta vào Firewall/Rules/LAN để tạo rule mới.

A screenshot of a computer

Description automatically generated

Kết quả:

Máy Windows 10 trong mạng LAN vẫn tìm kiếm được từ khoá facebook nhưng khi truy cập vào facebook.com thì không truy cập được

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### 3.4.2. Cài đặt Snort trên pfsense để ngăn chặn bypass

Để cài đặt Snort ta voà System/ Package Manager/ Available Packages

Tìm kiếm Snort và bấm Install

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Bắt đầu thiết lập chức năng trên interface, trường hợp này chọn card WAN, do muốn phát hiện và chặn trên đường truyền WAN.

A screenshot of a computer

Description automatically generated

* Block Offenders: Snort sẽ **tự động block IP** nếu phát hiện packet vi phạm rules
* Legacy Mode: Snort chỉ xem bản sao packet
* Kill States: Ngắt kết nối hiện tại từ IP bị chặn
* Which IP to Block: BOTH Block cả IP nguồn và IP đích

Sang tab WAN Categories để bật các nhóm rules.

A screenshot of a computer

Description automatically generated

Để chặn một số kĩ thuật bypass như gửi các gói phân mảnh, sproofed source thì ta sẽ tick chọn các rule như:

* decoder.rules: Phát hiện lỗi/biến dạng trong packet header (phân mảnh bất thường, TTL 0, checksum sai...)
* frag3-engine.rules: Phát hiện các gói phân mảnh bất thường như tiny fragment, overlap fragment – kỹ thuật Nmap -f
* bad-traffic.rules: Phát hiện các gói có IP spoof, source port = 0, địa chỉ loopback hoặc reserved
* preprocessor.rules: Giám sát hành vi không tuân chuẩn TCP/IP hoặc cố tình evade detection
* emerging-scan.rules: Phát hiện các loại scan như Nmap NULL, XMAS, FIN, decoy scan, stealth scan
* emerging-netbios.rules: Phát hiện scan hoặc exploit qua giao thức NetBIOS có thể dùng phân mảnh
* policy.rules: Phát hiện các gói sai chuẩn RFC – gói trống flag, không checksum, hành vi bất thường
* dos.rules: Tấn công từ chối dịch vụ qua phân mảnh chồng lấn, fragment flood, malformed packets
* backdoor.rules: Phát hiện mã độc hoặc C2 giao tiếp dùng source port bất thường như 53, 20, hoặc phân mảnh payload
* experimental.rules: Các rule đang thử nghiệm để phát hiện kỹ thuật evade hoặc tunneling nâng cao.

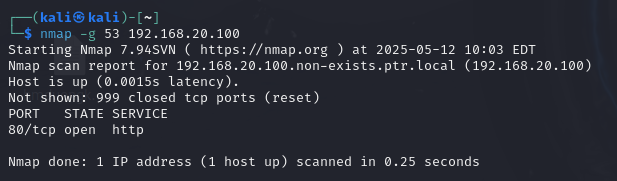
|  |
| --- |
| * emerging-policy.rules: Phát hiện traffic trái phép (giả mạo DNS, NTP...) |

Trước khi áp dụng rule:

A screen shot of a computer code

Description automatically generated

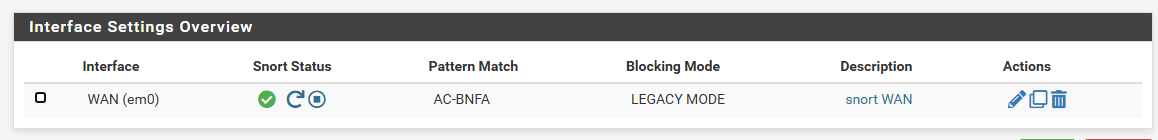
A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Sau khi áp dụng rule:



A computer screen shot of white text

Description automatically generated

A screen shot of a computer code

Description automatically generated

A screen shot of a computer code

Description automatically generated

### 3.4.3. Cài đặt OpenVPN trên PFsense (2.7.2) và cấu hình Client-To-Site

Trước khi cài đặt, ta kiểm tra ping từ máy Client tới Pfsense (192.168.38.128) và mạng LAN (192.168.10.1)

A screenshot of a computer program

Description automatically generated

Tiến hành tạo CA và Certificate trên máy Win 10 ở mạng LAN để xác thực người dùng và server.

Vào Web GUI của pfsense và vào System/ Certificte/ Authorities

A screenshot of a computer

Description automatically generated

Chọn Add để tạo CA (Certificate Authority) mới

A screenshot of a computer

Description automatically generated

* Descriptive name: pfsense\_rootca
* Method: chọn Create an internal certificates authority
* Trust Store: có thể chọn
* Các thiết lập tại Internal Certificate Authority có thể tùy chọn hoặc bỏ qua (để trống)

A screenshot of a computer

Description automatically generated

Tiếp theo chuyển sang tab Certificates để tạo Sign mới cho OpenVPN. Chọn Add/Sign

A screenshot of a computer

Description automatically generated

* Method: chọn Create an internal certificates
* Descriptive name: vpn\_ser\_cert
* Certificate authority: chọn CA vừa tạo ban nãy (pfsense\_rootca)
* Common Name: 192.168.38.128
* Certificate Type: Server Certificates

A screenshot of a computer

Description automatically generated

Tiếp theo ta tiến hành cấu hình OpenVPN. Vào VPN/ OpenVPN/ Wizards

A screenshot of a computer

Description automatically generated

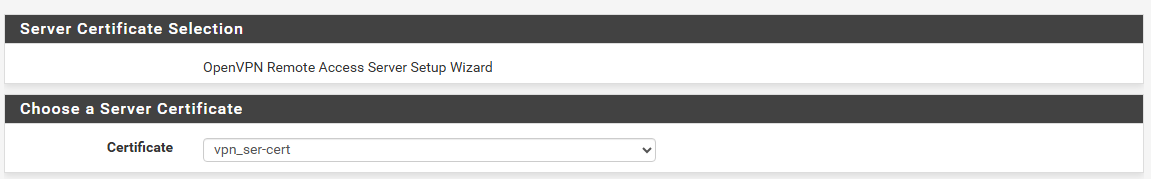
Ta bấm Next

A screenshot of a computer

Description automatically generated

* Certificate Authority: pfsense\_rootca

Ta bấm Next



* Certificate: vpn\_ser-cert

Ta bấm Next

A screenshot of a computer

Description automatically generated

* Description: remote user
* IPv4 Tunnel Network: 10.0.0.0/24
* Redirect IPv4 Gateway: check
* IPv4 Local Network: IP LAN
* Concurrent Connections: 5
* Advanced client settings: bỏ qua

Next và check 2 tuỳ chọn như bên dưới

A close up of a text

Description automatically generated

Vậy là ta đã cấu hình xong phần server cho OpenVPN

A screenshot of a computer

Description automatically generated

Tiếp theo ta sang tab Clients để cấu hình client cho OpenVPN

A screenshot of a computer

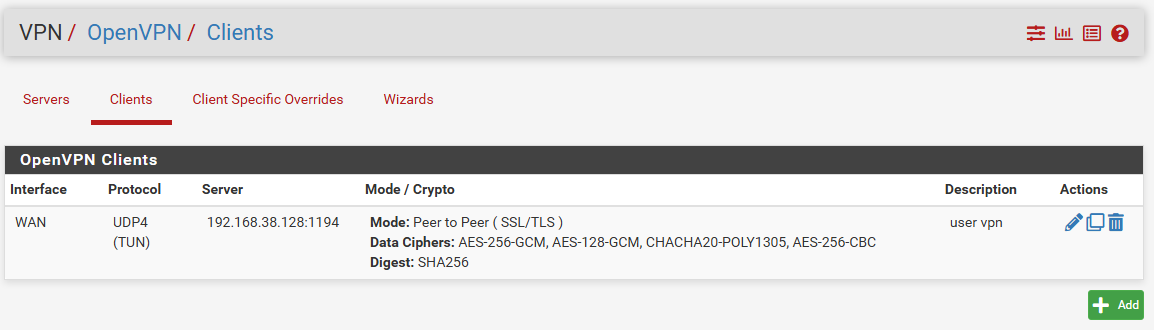
Description automatically generated

Chọn Add

A screenshot of a computer

Description automatically generated

* Description: user vpn
* Server host or address: IP WAN
* Nhập Username: vpn và Password: 123456
* Gateway creation: IPv4 only
* Chọn SAVE và hoàn tất



Tiếp theo ta tạo user trong System/ User Manager/ Users để phân quyền

A screenshot of a computer

Description automatically generated

Chọn Add

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Nhập Username và Password như trên
* Chọn ô Certificate và nhập như hình

**A screenshot of a computer

Description automatically generated**

* User này dùng để export cấu hình của OpenVPN

Tiếp theo ta tải gói “openvpn-client-export” tại System/ Package Manager/ Available Package

A screenshot of a computer

Description automatically generated

* Tìm kiếm “openvpn-client-export” và bấm Install

Sau khi cài đặt xong trong VPN/ OpenVPN sẽ có tab Client Export. Ở dưới sẽ có các bản cài đặt cho Client

A screenshot of a computer

Description automatically generated

Tải bản cần cài đặt và chuyển file sang máy Client (WAN).

Tiến hành cài đặt trên máy Client (WAN).

A screenshot of a computer

Description automatically generated

* Chọn Install

Khởi chạy và kết nối

Đăng nhập tài khoản vừa tạo ban nãy

A screenshot of a computer

Description automatically generated

Quá trình kết nối thành công sẽ hiển thị IP cấp cho VPN

A screenshot of a computer error

Description automatically generated

Kiểm tra lại trong Status/ OpenVPN sẽ thấy thông tin Client

A screenshot of a computer

Description automatically generated

Kiểm tra kết quả:

Máy Client có thể Ping tới mạng LAN

A computer screen with white text

Description automatically generated

Kiểm tra gói tin bằng Wireshark

A screenshot of a computer

Description automatically generated

* Các gói tin đã được mã hóa