**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

Viện Công nghệ thông tin và Truyền thông

A close up of a sign

Description automatically generated

**Firewall và các kiến trúc firewall**

***Nhóm 28***

1. Nguyễn Trung Nghĩa – 20173285

2. Nguyễn Nhật Tân - 20173355

3. Lưu Tuấn Linh – 20173233

4. Lương Duy Anh - 20172952

*Hà Nội, ngày tháng 05 năm* *2020*

Contents

[1. Firewall (tường lửa) là gì ? 3](#_Toc42513707)

[2. Phân loại Firewall 3](#_Toc42513708)

[3. Chức năng, thành phần và nguyên lí hoạt động của firewall 4](#_Toc42513709)

[3.1. Chức năng 4](#_Toc42513710)

[3.2 Các thành phần của Firewall và nguyên lý hoạt động 5](#_Toc42513711)

[3.2.1 Bộ lọc gói (Packet Filtering) 5](#_Toc42513712)

[3.2.2 Cổng ứng dụng (Appication-level Gateway) 6](#_Toc42513713)

[3.2.3. Cổng vòng (Circuit-level Gateway) 7](#_Toc42513714)

[4. Các kiến trúc Firewall 8](#_Toc42513715)

[4.1 Dual - Homed Host (máy chủ trung gian) 8](#_Toc42513716)

[4.2 Screened Host 10](#_Toc42513717)

[4.3 Screened subnet host 12](#_Toc42513718)

[4.4 Sử dụng nhiều Bastion Host 14](#_Toc42513719)

[4.5 Kiến trúc ghép chung Router trong (Interior Router) và Router ngoài (Exterior Router) 16](#_Toc42513720)

[4.6 Kiến trúc ghép chung Bastion Host và Router ngoài (Exterior Router) 16](#_Toc42513721)

[5. PfSense 18](#_Toc42513722)

[5.1 Giới thiệu PfSense 18](#_Toc42513723)

[5.2 Cài đặt máy ảo Window Server 2019 trên VMware 19](#_Toc42513724)

[5.3 Cài đặt PfSense trên một máy ảo khác 20](#_Toc42513725)

[5.4 Cấu hình trên máy Window server 25](#_Toc42513726)

[5.5 Chặn web và quảng cáo bằng PfSense 29](#_Toc42513727)

# Firewall (tường lửa) là gì ?

Firewall hay còn gọi là tường lửa, là một hệ thống an ninh mạng. Nó là một công cụ phần cứng hoặc phần mềm hoặc là cả 2 được tích hợp vào hệ thống để chống lại sự truy cập trái phép, ngăn chặn virus… để đảm bảo nguồn thông tin nội bộ được an toàn, tránh bị kẻ gian đánh cắp thông tin cũng như hạn chế sự xâm nhập vào hệ thống của một số thông tin khác không mong muốn.

Nói ngắn gọn và dễ hiểu hơn thì Firewall chính là ranh giới bảo mật giữa bên trong và bên ngoài của một hệ thống mạng máy tính.

Tường lửa (Firewall) sẽ đảm bảo rằng máy tính được bảo vệ từ hầu hết các mối tấn công nguy hại phổ biến. Và máy tính nào khi kết nối tới Internet cũng cần có firewall, điều này giúp quản lý những gì được phép vào mạng và những gì được phép ra khỏi mạng.

# Phân loại Firewall

Firewall có thể là một thiết bị phần cứng chuyên dụng hoặc có thể là một sản phẩm phần mềm được cài trên một máy chủ làm nhiệm vụ như một firewall hoặc cũng có thể là một ứng dụng được cài trên máy tính cá nhân. Việc phân loại firewall có thể có nhiều cách khác nhau, tuy nhiên ta có thể phân loại nó thành 1 trong 2 loại sau

**Personal Firewall:** Loại này được thiết kế để bảo vệ một máy tính trước sự truy cập trái phép từ bên ngoài. Bên cạnh đó thì Personal Firewall còn được tích hợp thêm tính năng như theo dõi các phần mềm chống virus, phần mềm chống xâm nhập để bảo vệ dữ liệu. Một số Personal Firewall thông dụng như: Microsoft Internet connection firewall, Symantec personal firewall, Cisco Security Agent…. Loại Firewall này thì thích hợp với cá nhân bởi vì thông thường họ chỉ cần bảo vệ máy tính của họ, thường được tích hợp sẵn trong máy tính Laptop, máy tính PC..

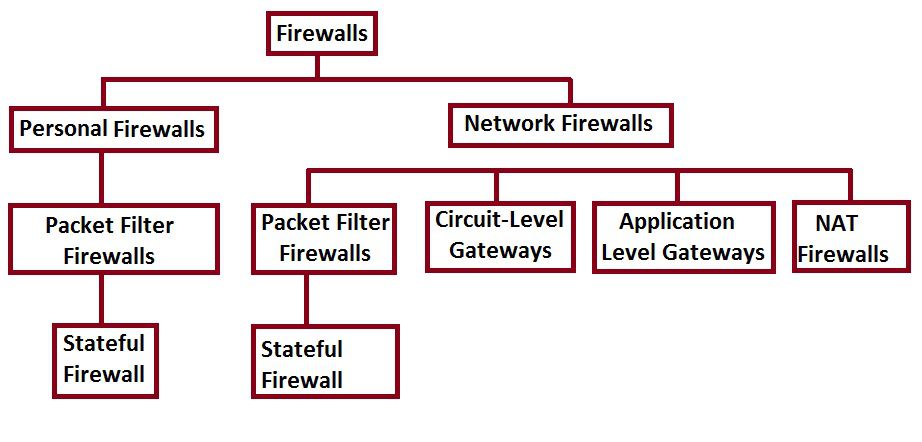
**Network Firewalls:** Được thiết kế ra để bảo vệ toàn bộ một hệ thống mạng máy tính trước sự tấn công từ bên ngoài, do đó Network Firewall cần phải được thiết kế và xây dựng với những chức năng chuyên biệt hơn nhằm phục vụ tốt hơn công việc của nó. Chúng ta có các ***Appliance-Based network Firewalls*** (Firewall dựa trên nền tảng phần cứng) như *Cisco PIX, Cisco ASA, Juniper NetScreen firewall, Nokia firewalls, Symantec’s Enterprise Firewall*. Hoặc một số ví dụ về **Software-Base firewalls** (Firewall dựa trên nền tảng phần mềm) như *Check Point’s Firewall, Microsoft ISA Server, Linux-based IPTables*.

=>  Điểm khác nhau giữa 2 loại Firewall này đó là số lượng host được Firewall bảo vệ. Bạn hãy nhớ 1 điều là **Personal firewall** chỉ bảo vệ cho một máy duy nhất còn **Network firewall** lại khác, nó sẽ bảo vệ cho cả một hệ thống mạng máy tính.

Trong đó, hệ thống**Network Firewall** được cấu tạo bởi các thành phần chính như sau:

1. Bộ lọc Packet (Packet- Filtering Router)
2. Cổng ứng dụng (Application-Level Gateway hay Proxy Server).
3. Cổng vòng (Circuit-Level Gateway).

Các bạn nhìn vào sơ đồ bên dưới là có thể hình dung ra được 2 loại Firewalls trên:



# **Chức năng, thành phần và nguyên lí hoạt động của firewall**

## 3.1. Chức năng

Kiểm soát luồng thông tin giữa máy tính cá nhân/mạng nội bộ và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong và bên ngoài. Cụ thể:

- Cho phép hoặc cấm những dịch vụ truy nhập từ trong ra ngoài

- Cho phép hoặc cấm những dịch vụ truy nhập từ ngoài vào trong.

- Theo dõi luồng dữ liệu mạng giữa 2 bên.

- Kiểm soát địa chỉ truy nhập, cho phép/cấm địa chỉ truy nhập

- Kiểm soát người sử dụng và việc truy nhập của người sử dụng

- Kiểm soát nội dung thông tin lưu chuyển trên mạng.

## 3.2 Các thành phần của Firewall và nguyên lý hoạt động

### **3.2.1 Bộ lọc gói (Packet Filtering)**

- Nguyên lý hoạt động:

Bộ lọc gói hoạt động chặt chẽ với giao thức TCP/IP ở tầng giao vận vì dữ liệu của các dịch vụ trên tầng ứng dụng (DNS, HTTP, FTP, SMTP,…) gửi xuống tầng giao vận sẽ được chia nhỏ thành các gói dữ liệu (data packet) rồi gán cho thông tin cần thiết(header) để có thể nhận dạng và tái lập lại các gói thành dữ liệu hoàn chỉnh ở đích cần gửi đến.

Bộ lọc gói cho phép hay từ chối những gói mà nó nhận được. Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thỏa mãn một trong số các luật lệ của lọc gói hay không. Các luật lọc gói dựa trên thông tin ở đầu các gói (packet header), dùng để cho phép truyền các packet đó trên mạng. Đó là:

+ Địa chỉ IP nguồn (IP Source Address)

+ Địa chỉ IP đích (IP Destination Address)

+ Giao thức truyền tin (TPC, UDP, ICMP,…)

+ Địa chỉ cổng nguồn (TCP/UDP source port)

+ Địa chỉ cổng đích (TCP/UDP destination port)

+ Dạng thông báo ICMP (ICMP message type)

+ Cổng gói tin đến (Incomming interface of packet)

+ Cổng gói tin đi (Outcoming interface of packet)

Nếu luật lệ lọc gói tin được thỏa mãn thì gói tin được chuyển qua firewall, nếu không gói tin sẽ bị bỏ đi.  Nhờ vậy mà firewall có thể ngăn cản được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khóa việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép. Ngoài ra, việc kiểm soát các cổng làm cho firewall có khả năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó hoặc những dịch vụ nào đó (SSH, SMTP, FTP…) được phép mới chạy được trên hệ thống mạng cục bộ.

- Ưu điểm và nhược điểm:

+ Ưu điểm:

Đa số các hệ thống firewall đều được sử dụng bộ lọc gói tin. Một trong những ưu điểm của phương pháp dùng bộ lọc gói là chi phí thấp vì cơ chế lọc gói đã có sẵn trong các router.

Ngoài ra, bộ lọc gói là trong suốt đối với người sử dụng và các ứng dụng vì vậy nó không yêu cầu người sử dụng phải thao tác gì cả.

+ Nhược điểm:

Việc định nghĩa các chế độ lọc gói là một việc khá phức tạp, nó đòi hỏi người quản trị mạng cần có hiểu biết chi tiết về các dịch vụ internet, các dạng packet header. Khi yêu cầu về lọc gói tin càng lớn, các rules càng trở nên phức tạp do đó rất khó quản lý và điều khiển.

Do làm việc dựa trên header của các packet nên bộ lọc không kiểm soát được nội dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăn cắp thông tin hay phá hoại của kẻ xấu.

### **3.2.2 Cổng ứng dụng (Appication-level Gateway)**

- Nguyên lý hoạt động:

Đây là một loại firewall được thiết kế dể tăng cường chức năng kiểm soát các loại dịch vụ, giao thức truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là proxy service. Proxy service là các bộ code đặc biệt cài đặt trên cổng ra (gateway) cho từng ứng dụng. Nếu người quản trị mạng không cài đặt proxy service cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall. Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quản trị cho là chấp nhận được trong khi từ chối những đặc điểm khác.

Một cổng ứng dụng thường được coi như là một Bastion host (pháo đài) bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đảm bảo an ninh của một Bastion host là:

+ Bastion host luôn chạy các version an toàn (secure version) của các phần mềm hệ điều hành (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào hệ điều hành (Operating system) cũng như là đảm bảo sự tích hợp firewall.

+ Chỉ những dịch vụ mà người quản trị mạng cho là cần thiết mới được cài đặt trên Bastion host, đơn giản chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên Bastion host.

+ Bastion host có thể yêu cầu nhiều mức độ khác nhau ví dụ như username và password.

+ Mỗi proxy được cài đặt cấu hình để cho phép truy nhập chỉ một số các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

+ Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của dữ liệu mạng đi qua nó. Điều này có nghĩ là bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

+ Mỗi proxy đều độc lập với các proxy khác trên Bastion host. Điều này cho phép dễ dàng cài đặt một proxy mới hay tháo gỡ một proxy.

- Ưu điểm và nhược điểm:

+ Ưu điểm:

Cho phép người quản trị hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy cập bởi các dịch vụ.

Cho phép người quản trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì nếu không thấy các proxy cho các dịch vụ tương ứng có nghĩa là dịch vụ ấy bị khóa.

Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt và nó có nhậy ký ghi chép lại thông tin về truy cập hệ thống.

Rule lọc cho cổng ứng dụng dễ dàng cấu hình và kiểm tra hơn so với bộ lọc gói.

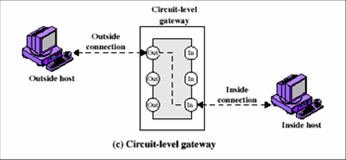
+ Nhược điểm:

Cần phải có sự cấu hình trên máy user để user truy cập vào các dịch vụ proxy. Ví dụ telnet.

### **3.2.3. Cổng vòng (Circuit-level Gateway)**

Circuit Level Gateway – cổng vòng – là một chức năng đặc biệt có thể thực hiện bởi một cổng ứng dụng. Cổng vòng đơn giản chỉ là chuyển tiếp các kết nối TCP mà không thực hiện bất kì một hành động xử lý hay lọc gói nào.

Minh họa một hành động sử dụng kết nối telnet qua cổng vòng. Cổng vòng đơn giản chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục telnet nào. Cổng vòng làm việc như một sợi dây, sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên vì sự kết nối này xuất hiện từ hệ thống firewall nên nó che dấu thông tin về mạng nội bộ.

[](https://argron.files.wordpress.com/2012/09/image_thumb4.png)

Circuit-level Gateway

Cổng vòng thường được sử dụng cho những kết nối ra ngoài. Ưu điểm lớn nhất là một Bastion host có thể được cấu hình như là một hỗn hợp cung cấp cổng ứng dụng cho những kết nối đến và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống firewall dễ dàng sử dụng cho người dùng trong mạng nội bộ muốn trực tiếp truy câp tới các dịch vụ internet, trong khi vẫn cung cấp chức năng bảo vệ mạng nội bộ từ những sự tấn công bên ngoài.

1. Các kiến trúc Firewall

## 4.1 Dual - Homed Host (máy chủ trung gian)

Dual Homed Host là kiến trúc được xây dựng và phát triển dựa trên một thiết bị có 2 network interface trở lên, có nghĩa là máy đó có gắn hai card mạng giao tiếp với hai mạng khác nhau: một nối với mạng nội bộ (LAN) và một nối với mạng ngoài (Internet), như thế máy tính này đóng vai trò là router phần mềm.

Dual-homed host chỉ có thể cung cấp các dịch vụ bằng cách ủy quyền(proxy) chúng hoặc cho phép users đăng nhập trực tiếp vào Dual-homed host. Do đó mà các hệ thống bên trong và bên ngoài của kiến trúc không thể giao tiếp trực tiếp với nhau. Để làm việc được với một máy trên Internet, người dùng ở mạng cục bộ trước hết phải login vào Dual–homed Host, và từ đó bắt đầu phiên làm việc. Tất cả quá trình trao đổi thông tin được diễn ra thông qua những dữ liệu được chia sẻ trên máy Dual – homed.

Kiến trúc này có một đặc điểm đó chính là mọi dữ liệu muốn đi qua nó thì cần phải có một phần mềm đặc biệt có khả năng chuyển những yêu cầu ứng dụng giữa hai mạng đã được kết nối với nhau hay còn gọi là Application forwarder. Loại kiến trúc này thường được ứng dụng chủ yếu trong các trường hợp những dữ liệu được dùng để trao đổi ra bên ngoài và không mang tính quan trọng hay cấp thiết.

Ưu điểm của Dual – homed Host:

* Nó có thể tách một mạng bên trong ra khỏi những mạng được coi là mạng không tin cậy. Đồng thời, nó không truyền đi bất cứ IP nào nên có khả năng ngăn chặn một cách tuyệt đối nguồn dữ liệu IP giữa những mạng không tin cậy bên trong và bên ngoài.
* Cài đặt dễ dàng, không yêu cầu phần cứng hoặc phần mềm đặc biệt.
* Dual–homed Host chỉ yêu cầu cấm khả năng chuyển các gói tin, do vậy, thông thường trên các hệ Unix, chỉ cần cấu hình và dịch lại nhân (Kernel) của hệ điều hành là đủ.

Nhược điểm của Dual–homed Host:

* Không đáp ứng được những yêu cầu bảo mật ngày càng phức tạp, cũng như những hệ phần mềm mới được tung ra thị trường.
* Không có khả năng chống đỡ những cuộc tấn công nhằm vào chính bản thân nó, và khi Dual–homed Host đó bị đột nhập, nó sẽ trở thành đầu cầu lý tưởng để tấn công vào mạng nội bộ.
* Nếu như hệ thống hoạt động cùng lúc quá nhiều ứng dụng thì sẽ dẫn đến hiện tượng quá tải toàn hệ thống. Lúc này, khả năng rủi ro cũng tăng cao khi tường lửa bị tấn công từ bên ngoài và có thể dẫn đến nguy cơ tất cả các host trong mạng cũng bị tấn công.

**Đánh giá về kiến trúc Dual–homed Host:**

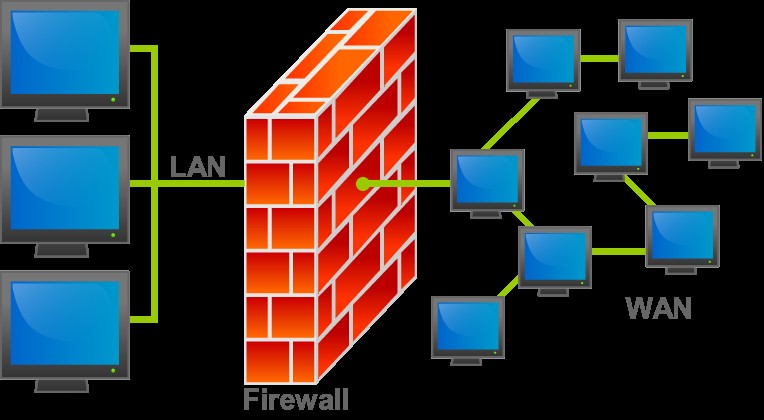
Để cung cấp dịch vụ cho những người sử dụng internal network có một số giải pháp như sau:

* Kết hợp với các Proxy Server cung cấp những Proxy Service
* Cấp các account cho user trên máy dual–homed host này và khi mà người sử dụng muốn sử dụng dịch vụ từ Internet hay dịch vụ từ external network thì họ phải logging in vào máy này.

Nếu dùng phương pháp cấp account cho user trên máy dual– homed host thì user không thích sử dụng dịch vụ phiền phức như vậy, vì mỗi lần họ muốn sử dụng dịch vụ thì phải loging in vào máy khác (dual homed host) khác với máy của họ đây là vấn đề rất là không trong suốt với người sử dụng.

Nếu dùng Proxy Server : Khó có thể cung cấp được nhiều dịch vụ cho người sử dụng vì phần mềm Proxy Server và Proxy Client không phải loại dịch vụ nào cũng có sẵn. Hoặc khi số dịch vụ cung cấp nhiều thì khả năng đáp ứng của hệ thống có thể giảm xuống vì tất cả các Proxy Server đều đặt trên cùng một máy.

Một khuyết điểm cơ bản của hai mô hình trên nữa là: khi mà máy dual –homed host nói chung cũng như các Proxy Server bị đột nhập vào. Người tấn công (attacker) đột nhập vào được qua nó thì lưu thông bên trong internal network bị attacker này thấy hết điều này thì hết sức nguy hiểm . Trong các hệ thống mạng dùng Ethernet hoặc Token Ring thì dữ liệu lưu thông trong hệ thống có thể bị bất kỳ máy nào nối vào mạng đánh cắp dữ liệu cho nên kiến trúc trên chỉ thích hợp với một số mạng nhỏ .

Dual Homed Host

## 4.2 Screened Host

Kiến trúc này kết hợp 2 kỹ thuật đó là Packet Filtering và Proxy Services.

Packet Filtering:

Bastion host được đặt bên trong mạng nội bộ Packet Filtering được cài trên router. Theo cách này, Bastion host là hệ thống duy nhất trong mạng nội bộ mà những host trên internet có thế kết nối tới. Mặc dù vậy, chỉ những kiểu kết nối phù hợp (được thiết lập trong Bastion host) mới được phép kết nối.

Bất kì một hệ thống bên ngoài nào cố gắng truy cập vào hệ thống hoặc các dịch vụ bên trong đều phải kết nối tới host này. Vì thế, Bastion host là host cần phải được duy trì ở chế độ bảo mật cao. Packet Filtering cũng cho phép Bastion host có thể mở kết nối ra bên ngoài.

Lọc một số loại dịch vụ mà hệ thống muốn cung cấp sử dụng Proxy Server, bắt người sử dụng nếu muốn dùng dịch vụ thì phải kết nối đến Proxy Server mà không được bỏ qua Proxy Server để nối trực tiếp với mạng bên trong/bên ngoài (internal/external network), đồng thời có thể cho phép Bastion Host mở một số kết nối với internal/external host.

Cấu hình của Packet Fiitering trên Screening router như sau:

- Cho phép tất cả các host bên trong mở kết nối tới host bên ngoài thông qua một số dịch vụ có định.

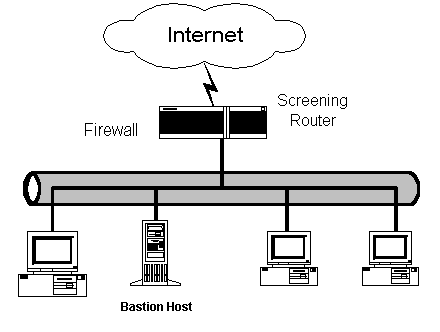
- Không cho phép tất cả các kết nối từ host bên trong (cấm những host này sử dụng proxy thông qua Bastion host).

- Bạn có thể kết hợp nhiều lối vào cho những dịch vụ khác nhau.

- Một số dịch vụ được phép đi vào trực tiếp qua packet filtering

- Một số dịch vụ khác thì chỉ được phép đi vào gián tiếp qua proxy

Proxy Service: Bastion Host sẽ chứa các Proxy Server để phục vụ một số dịch vụ hệ thống cung cấp cho người sử dụng qua Proxy Server.



*Hình 37: Sơ đồ kiến trúc Screened Host*

**Đánh giá một số ưu, khuyết điểm chính của kiến trúc Screened Host**

Kiến trúc screened host hay hơn kiến trúc dual–homed host ở một số điểm cụ thể sau:

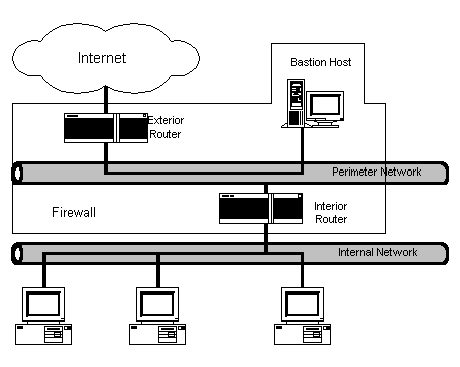
Dual–Homed Host: Khó có thể bảo vệ tốt vì máy này cùng lúc cung cấp nhiều dịch vụ, vi phạm qui tắc căn bản là mỗi phần tử hay thành phần nên giữ ít chức năng nếu có thể được (mỗi phần tử nên giữ ít chức năng càng tốt), cũng như tốc độ đáp ứng khó có thể cao vì cùng lúc đảm nhận nhiều chức năng.

Screened Host: Đã tách chức năng lọc các gói IP và các Proxy Server ở hai máy riêng biệt. Packet Filtering chỉ giữ chức năng lọc gói nên có thể kiểm soát, cũng như khó xảy ra lỗi (tuân thủ qui tắc ít chức năng). Proxy Servers được đặt ở máy khác nên khả năng phục vụ (tốc độ đáp ứng) cũng cao.

Cũng tương tự như kiến trúc Dual–Homed Host khi mà Packet Filtering system cũng như Bastion Host chứa các Proxy Server bị đột nhập vào (người tấn công đột nhập được qua các hàng rào này) thì lưu thông của internal network bị người tấn công thấy.

Từ khuyết điểm chính của 2 kiến trúc trên ta có kiến trúc thứ 3 sau đây khắc phục được phần nào khuyết điểm trên .

## 4.3 Screened subnet host



*Hình 38: Sơ đồ kiến trúc Screened Subnet Host*

Kiến trúc Screened subnet dẫn xuất từ kiến trúc Screened host bằng cách thêm vào phần an toàn: mạng ngoại vi (perimeter network) nhằm cô lập mạng nội bộ ra khỏi mạng bên ngoài, tách bastion host ra khỏi các host thông thường khác.

Với kiến trúc này, hệ thống này bao gồm hai Packet–Filtering Router và một Bastion Host (hình 38). Kiến trúc này có độ an toàn cao nhất vì nó cung cấp cả mức bảo mật: Network và Application trong khi định nghĩa một mạng perimeter network. Mạng trung gian (DMZ) đóng vai trò như một mạng nhỏ, cô lập đặt giữa Internet và mạng nội bộ. Cơ bản, một DMZ được cấu hình sao cho các hệ thống trên Internet và mạng nội bộ chỉ có thể truy nhập được một số giới hạn các hệ thống trên mạng DMZ, và sự truyền trực tiếp qua mạng DMZ là không thể được.

Kiểu Screened subnet đơn giản bao gồm hai Screened router

Với những thông tin đến, Router ngoài (Exterior Router) chống lại những sự tấn công chuẩn (như giả mạo địa chỉ IP), và điều khiển truy nhập tới DMZ. Nó chỉ cho phép hệ thống bên ngoài truy nhập Bastion Host. Router trong (Interior Router) cung cấp sự bảo vệ thứ hai bằng cách điều khiển DMZ truy nhập mạng nội bộ chỉ với những truyền thông bắt đầu từ Bastion Host.

Với những thông tin đi, Router trong điều khiển mạng nội bộ truy nhập tới DMZ. Nó chỉ cho phép các hệ thống bên trong truy nhập Bastion. Quy luật Filtering trên Router ngoài yêu cầu sử dụng dịch vụ Proxy bằng cách chỉ cho phép thông tin ra bắt nguồn từ Bastion Host.

Ưu điểm:

• Kẻ tấn công cần phá vỡ ba tầng bảo vệ: Router ngoài, Bastion Host và Router trong.

• Bởi vì Router ngoài chỉ quảng bá DMZ Network tới Internet, hệ thống mạng nội bộ là không thể nhìn thấy (invisible). Chỉ có một số hệ thống đã được chọn ra trên DMZ là được biết đến bởi Internet qua routing table và

DNS information exchange ( Domain Name Server ).

• Bởi vì Router trong chỉ quảng cáo DMZ Network tới mạng nội bộ, các hệ thống trong mạng nội bộ không thể truy nhập trực tiếp vào Internet. Điều nay đảm bảo rằng những user bên trong bắt buộc phải truy nhập Internet qua dịch vụ Proxy.

**Đánh giá về kiến trúc Screened Subnet Host**:

Đối với những hệ thống yêu cầu cung cấp dịch vụ nhanh, an toàn cho nhiều người sử dụng đồng thời cũng như khả năng theo dõi lưu thông của mỗi người sử dụng trong hệ thống và dữ liệu trao đổi giữ các người dùng trong hệ thống cần được bảo vệ thì kiến trúc cơ bản trên phù hợp.

Để tăng độ an toàn trong internal network, kiến trúc screen subnet ở trên sử dụng thêm một mạng DMZ (DMZ hay perimeter network) để che phần nào lưu thông bên trong internal network. Tách biệt internal network với Internet.

Sử dụng 2 Screening Router : Exterior Router và Interior Router.

Áp dụng qui tắc dư thừa có thể bổ sung thêm nhiều mạng trung gian (DMZ hay perimeter network) càng tăng khả năng bảo vệ càng cao.

Ngoài ra, còn có những kiến trúc biến thể khác như: sử dụng nhiều Bastion Host, ghép chung Router trong và Router ngoài, ghép chung Bastion Host và Router ngoài.

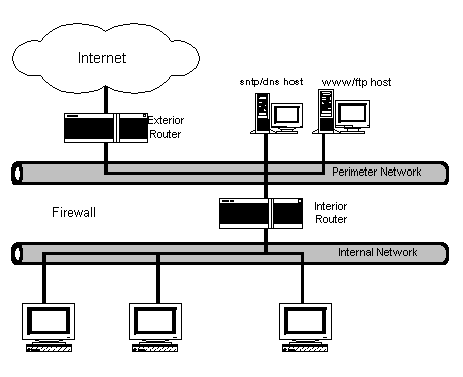
Screened Subnet

## 4.4 Sử dụng nhiều Bastion Host

Do các yêu cầu về tốc độ đáp ứng (performance) và dư thừa (redundancy), cũng như tách biệt các Servers khác nhau.

Sử dụng 1 Bastion Host cung cấp những dịch vụ cho người sử dụng bên trong (internal user), như dịch vụ SNMP Server, Proxy Servers …

Sử dụng 1 Bastion Host khác cung cấp dịch vụ cho Internet hoặc những người sử dụng bên ngoài (external user) sẽ sử dụng. Như là Anonymous FTP Server mà Server này những người sử dụng bên trong (local users) không truy xuất đến.



*Hình 39: Sơ đồ kiến trúc sử dụng 2 Bastion Host*

Với cách này thì tốc độ đáp ứng cho những người sử dụng bên trong (local user) một phần nào đó không bị ảnh hưởng (bị làm chậm đi) bởi hoạt động của những người sử dụng bên ngoài (external users).

Cũng có thể sử dụng nhiều Bastion Host mà cung cấp cho 1 dịch vụ nào đó để tăng tốc độ đáp ứng (performance), nhưng việc này cũng khó cân bằng tải giữa các Server trừ khi đoán trước được mức độ sử dụng.

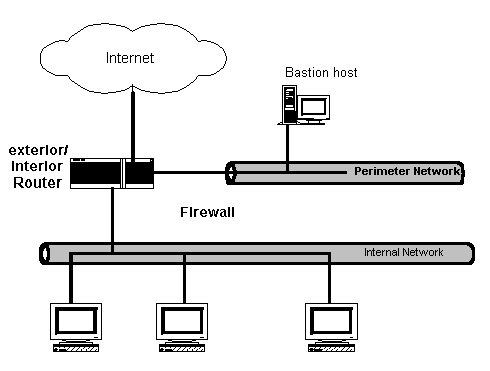
Việc sử dụng kỹ thuật dư thừa để đảm bảo tính sẵn sàng cao của hệ thống, để khi mà một Bastion Host hỏng thì có cái khác thay thế. Nhưng chỉ có một số loại dịch vụ trợ giúp dạng này: DNS Server, SMTP Server, ... có thể dùng nhiều Bastion Host làm DNS Server , SMTP Server. Khi một Bastion Host hỏng hoặc quá tải, những yêu cầu về DNS Server và SNMP sẽ được dùng qua Bastion Host khác như là một fallback system.

Sử dụng nhiều Bastion Host trong trường hợp muốn cung cấp dịch vụ cho nhiều mạng khác nhau, và loại dữ liệu cung cấp cho mỗi mạng cũng khác nhau.

Sử dụng nhiều Bastion Host cho các Server khác nhau để khi mà một Server nào đó bị đột nhập vào hay bị hỏng thì Server khác vẫn hoạt động tốt. Ví Dụ : Tách HTTP Server và FTP Server trên 2 máy riêng biệt.

## 4.5 Kiến trúc ghép chung Router trong (Interior Router) và Router ngoài (Exterior Router)

Sử dụng kiến trúc này thì cần tăng tốc độ của máy làm Router.

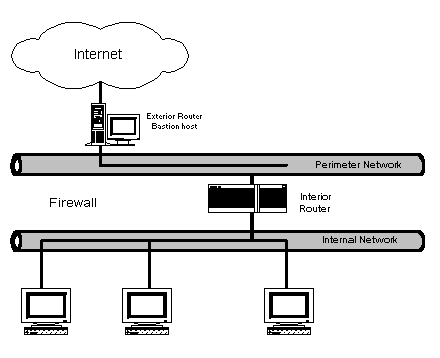


*Hình 40: Sơ đồ kiến trúc ghép chung Router trong và Router ngoài*

Kiến trúc này gần giống với Screened Host trong trường hợp khi mà exterior/interior Router bị đột nhập vào thì lưu thông trong mạng bên trong sẽ bị lộ ra bên ngoài nhưng tốt hơn Screened Host đó là nó cũng sử dụng thêm một mạng bên ngoài. Mạng bên ngoài sẽ chứa các Server có thể nối ra Internet mà nếu các Server này bị đột nhập thì lưu thông của mạng bên trong cũng không bị lộ ra bên ngoài. Kiến trúc này cũng gần giống với Screened Subnet nhưng mà exterior Router và interior Router được ghép chung nên nó giảm đi số lớp bảo vệ. Nói chung, kiến trúc ghép chung interior Router và exterior Router ở trung gian giữa hai kiến trúc này.

## 4.6 Kiến trúc ghép chung Bastion Host và Router ngoài (Exterior Router)

Kiến trúc này sử dụng cho mạng chỉ có một đường nối dùng nghi thức SLIP hoặc PPP ra Internet.



*Hình 41: Sơ đồ kiến trúc ghép chung Bastion Host và Router ngoài*

Kiến ghép chung Bastion Host và Router ngoài (Exterior Router) này gần giống với Screened Subnet. Nó cho tốc độ đáp ứng thường thấp nhưng mà vẫn có thể chấp nhận được do tốc độ đường truyền thấp, chức năng lọc của Router ngoài ít, chức năng lọc gói chủ yếu là Router trong.

# 5. PfSense

## 5.1 Giới thiệu PfSense

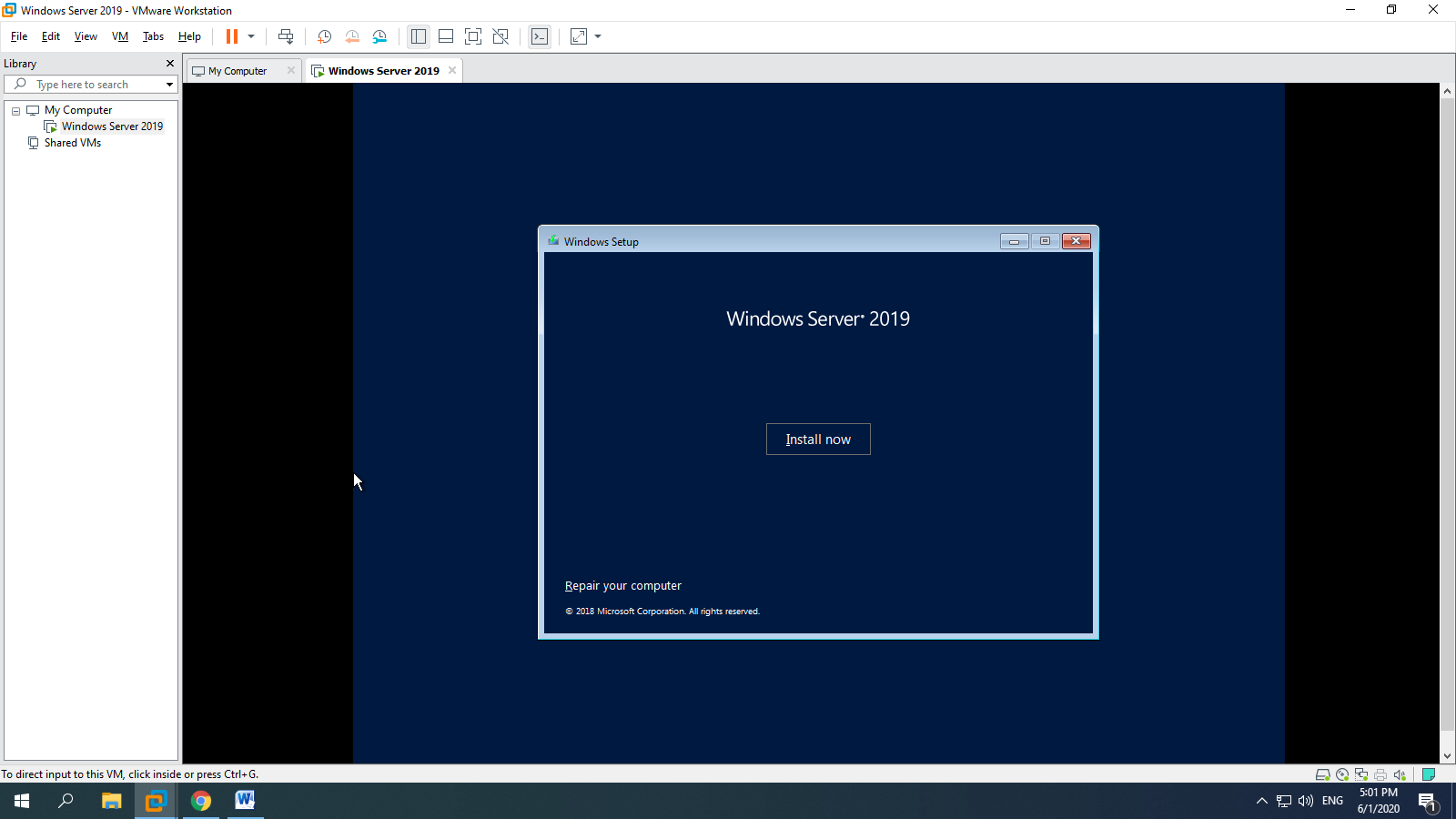
PfSene là một dự án nguồn mở dựa trên nền tảng hệ điều hành FreeBSD và được sử dụng như một tường lửa hoặc một thiết bị định tuyến. Chris Buechler và Scott Ullrich là hai tác giả sáng lập dự án m0n0wall năm 2004. Tuy nhiên tại thời điểm 2004, tác giả phải gặp vấn đề khó khăn khi mã nguồn của họ không tương thích tốt với các giải pháp tích hợp phần cứng (các thiết bị sử dụng 64MB RAM). PfSense với sự phát triển theo thời gian đã hỗ trợ rộng rãi các nền tảng phần cứng khác nhau và được sự đóng góp to lớn từ cộng động sử dụng mã nguồn mở thế giới. Cùng với các chức năng quản lý mạnh mẽ, thân thiện với người dùng nên pfSense được cộng đồng sử dụng rộng rãi trong môi trường doanh nghiệp vừa và nhỏ. PfSense yêu cầu cấu hình phần cứng thấp nên phù hợp cho việc tích hợp vào các thiết bị tích hợp khác nhau nhằm tăng tính linh động và hiệu suất trong quá trình vận hành.

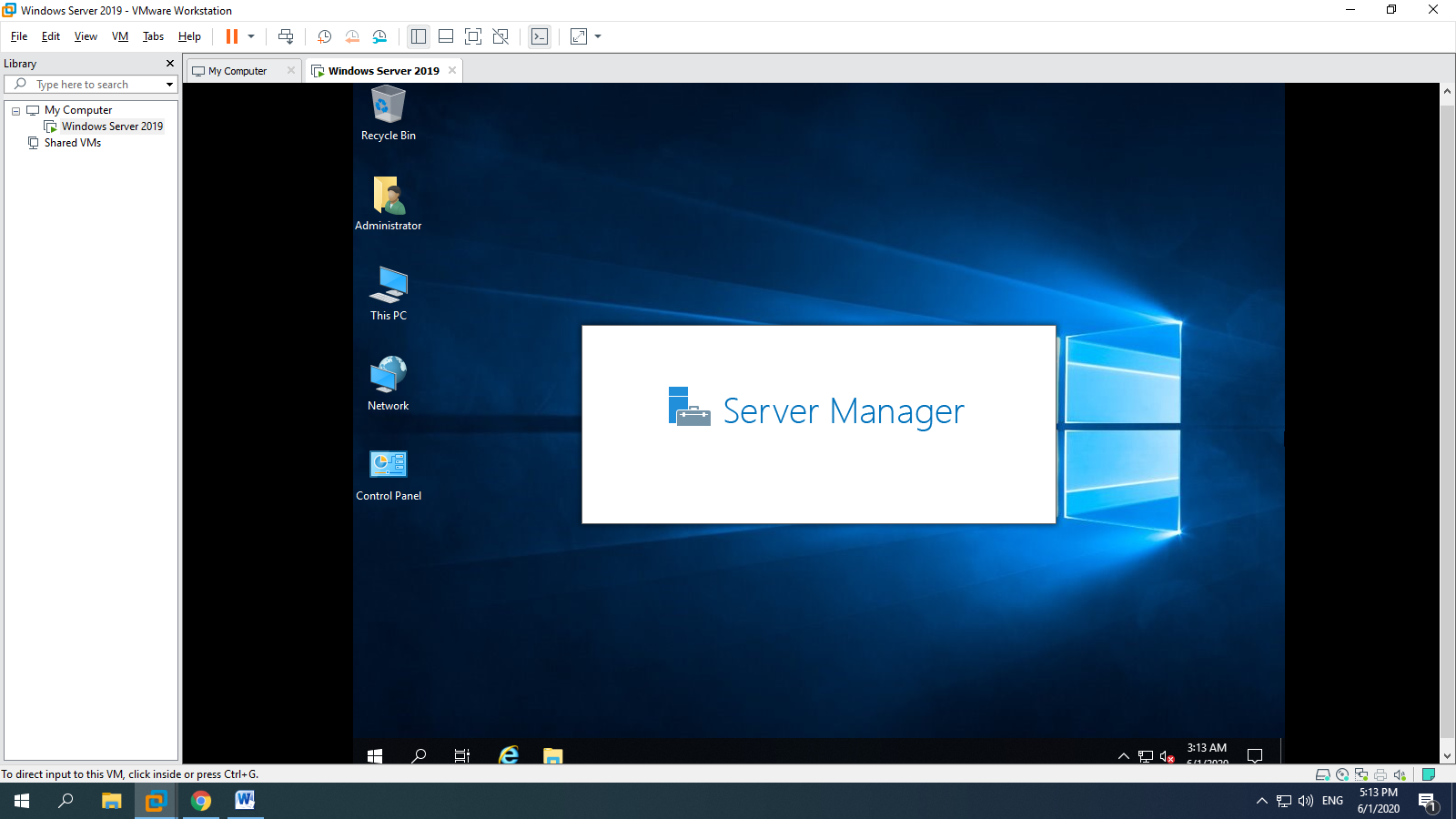
Phiên bản pfSense hiện tại được công bố là 2.1, tập trung phát triển các tính năng hỗ trợ môi trường mạng IPv6.

Với các tính năng linh hoạt, pfSense được sử dụng trong nhiều mục đích khác nhau trên thực tế. Giá thành triển khai thấp hơn so với những thiết bị cùng loại, hỗ trợ những tính năng cơ bản và nâng cao như VPN, BGP, Wirelsess, cân bằng tải, QoS… Các chức năng thường được sử dụng bao gồm:

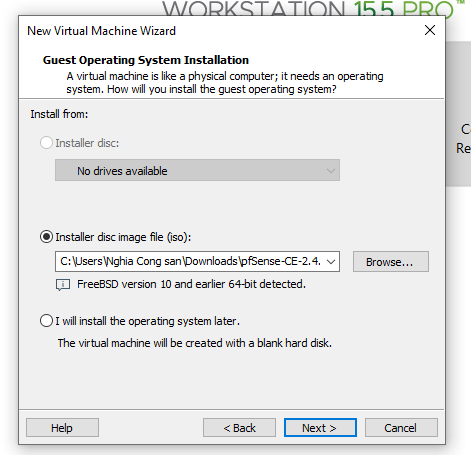
* Tường lửa: với tính năng xử lý gói tin TCP/IP mạnh mẽ, nên pfSense được dùng như một tường lửa nhằm cản lọc những kết nối không hợp pháp đến một phân vùng mạng chỉ định.
* Thiết bị định tuyến mạng WAN/LAN: đóng vai trò như một router, pfSense hỗ trợ các chức năng như định tuyến như PPoE, BGP… phù hợp cho doanh nghiệp triển khai với giá thành thấp mà không cần đầu tư thêm router cùng chức năng.Trong môi trường mạng LAN, pfSense hỗ trợ giao thức 802.1q cho phép nhân viên kỹ thuật có thể hoạch định các phân vùng mạng nội bộ khác nhau. PfSense có thể hỗ trợ băng thông 3Gbps hoặc xử lý hơn 500.000 gói tin/giây, vì vậy pfSense có thể sử dụng thay thế một thiết bị switch lớp 3 (yêu cầu có thêm card mạng).
* Wireless Access Point.
* Máy chủ VPN/DNS/DHCP/Sniffer: pfSense được tác giả tích hợp thêm các mã nguồn mở như TinyDNS (http://tinydns.org), tcpdump (http://www.tcpdump.org/) nhằm phục vụ với vai trò là máy chủ DNS hoặc máy chủ sniffer (thu thập gói tin cho nhiệm vụ phân tích).

## 5.2 Cài đặt máy ảo Window Server 2019 trên VMware





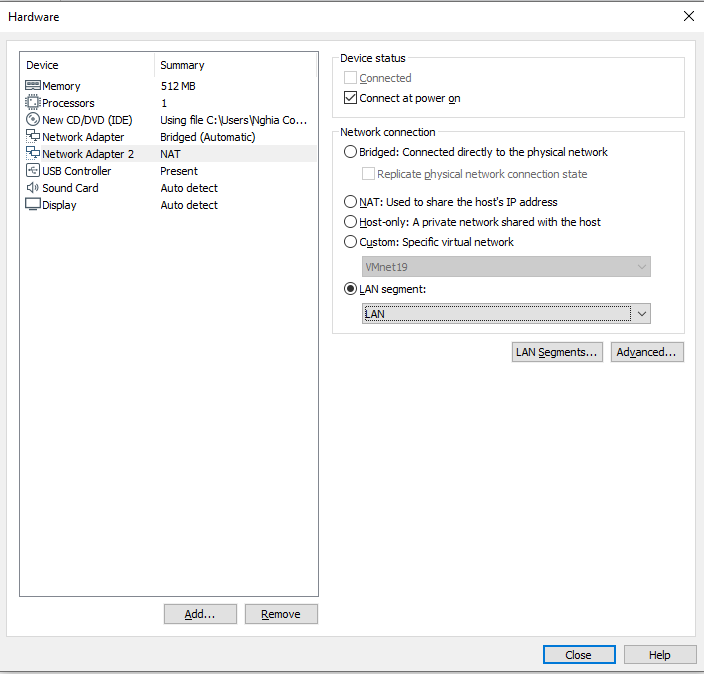
## 5.3 Cài đặt PfSense trên một máy ảo khác



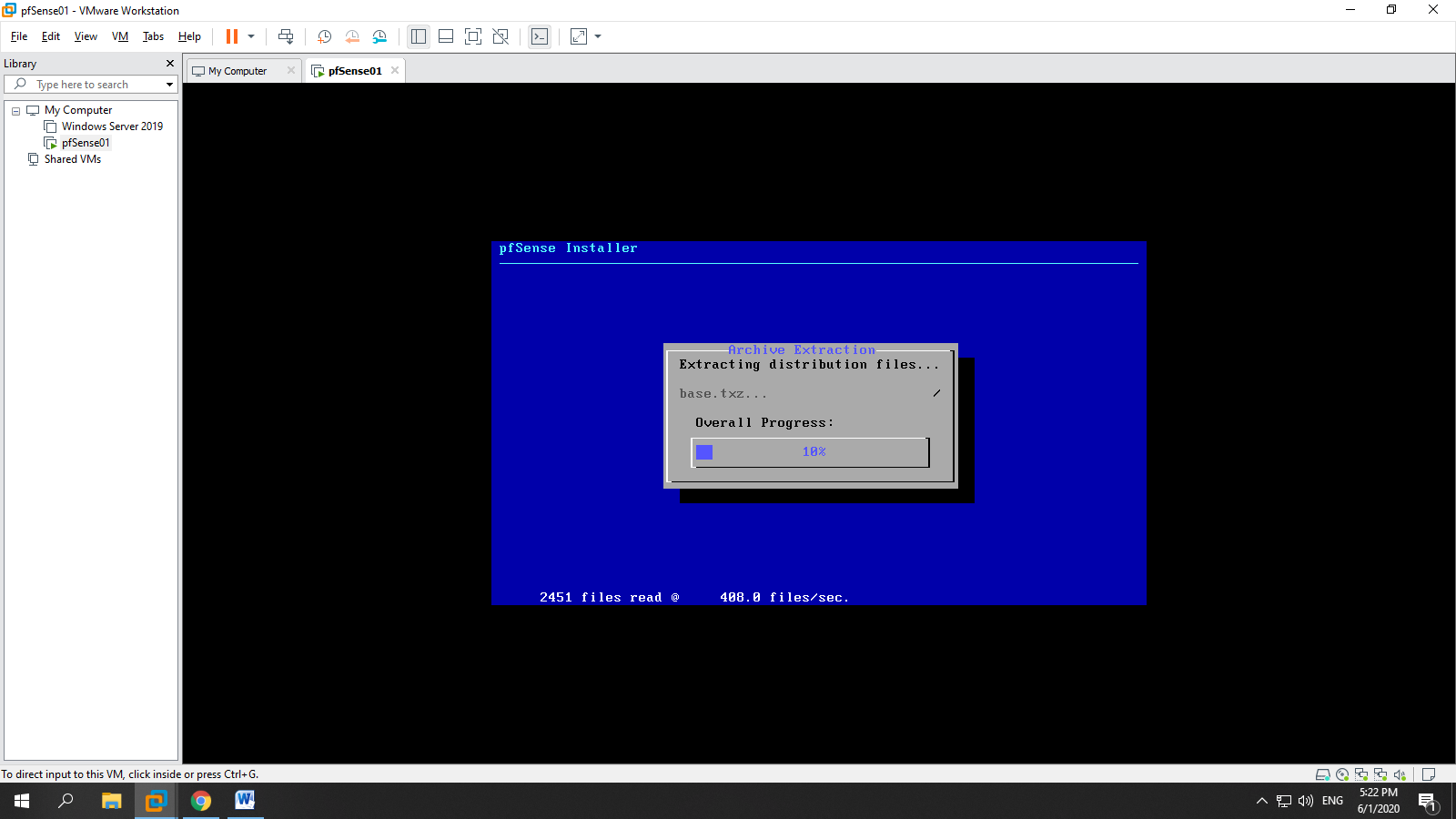
Cài đặt cấu hình cho máy ảo PfSense

2 card mạng:

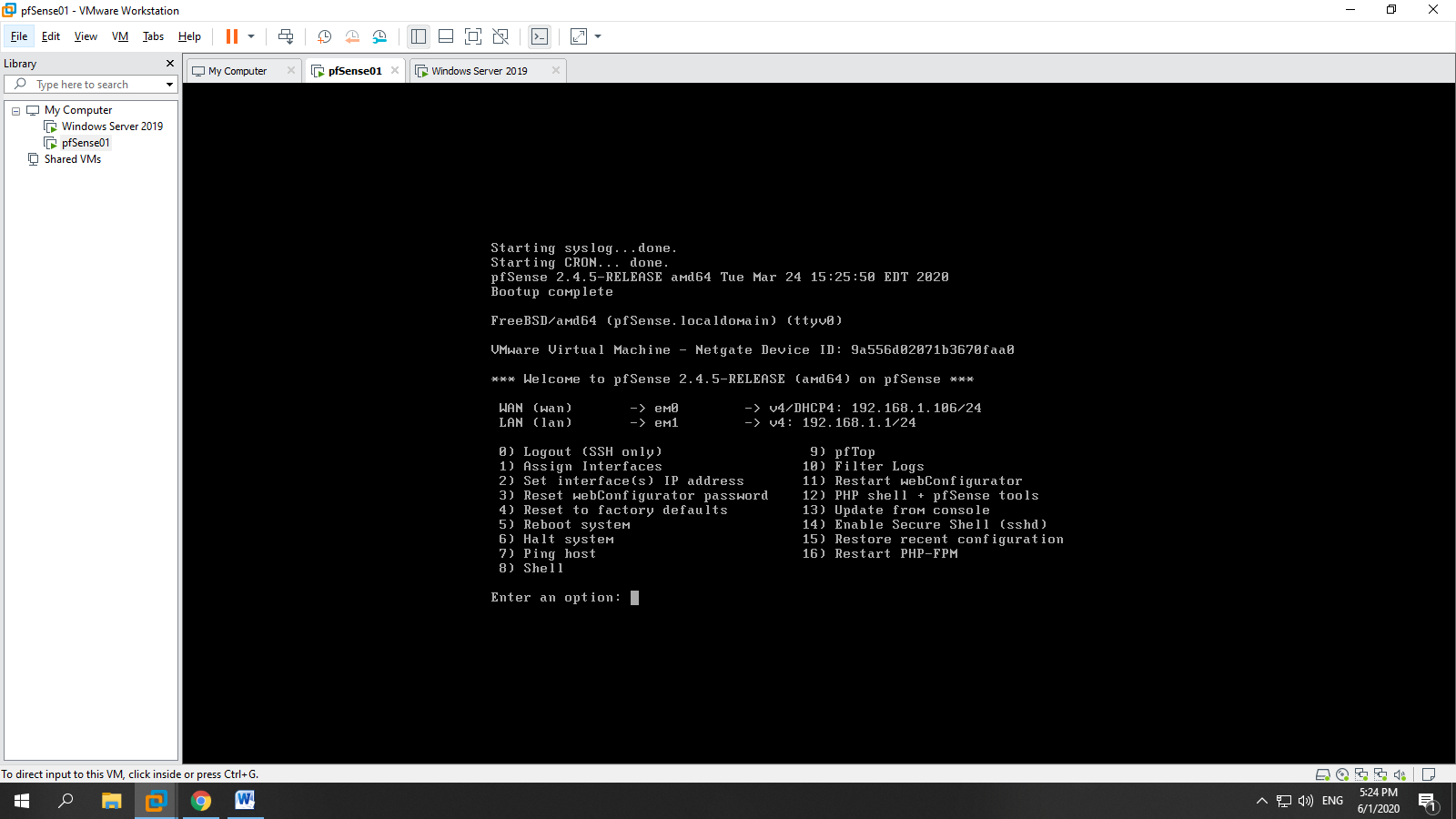
* Bridged dùng như 1 card WAN
* Card LAN



Bắt đầu cài đặt

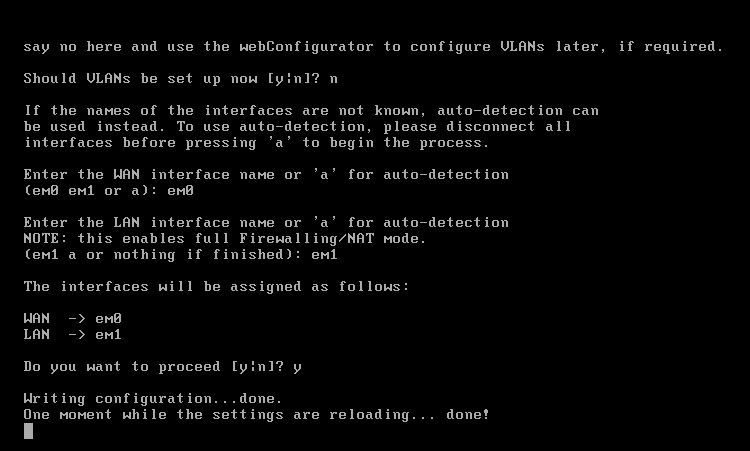


Sau khi cài đặt xong:

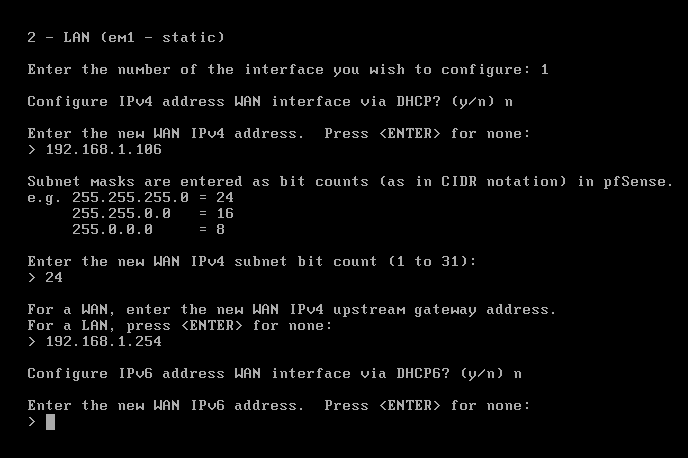


Địa chỉ card WAN giống địa chỉ IPv4 máy host

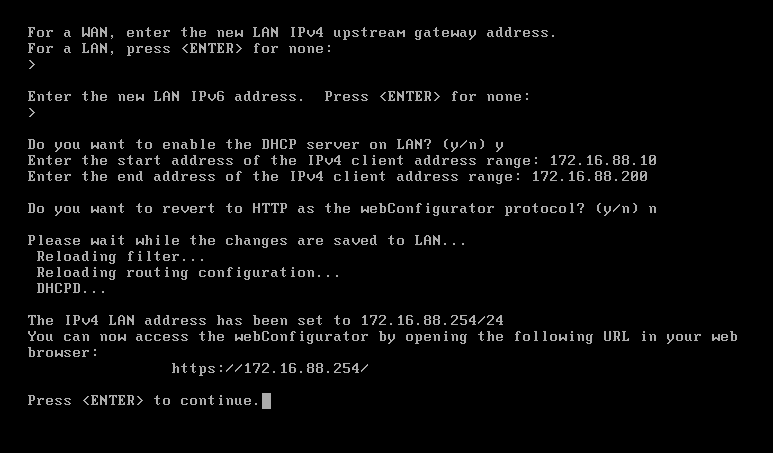
Tùy biến lại Interfaces



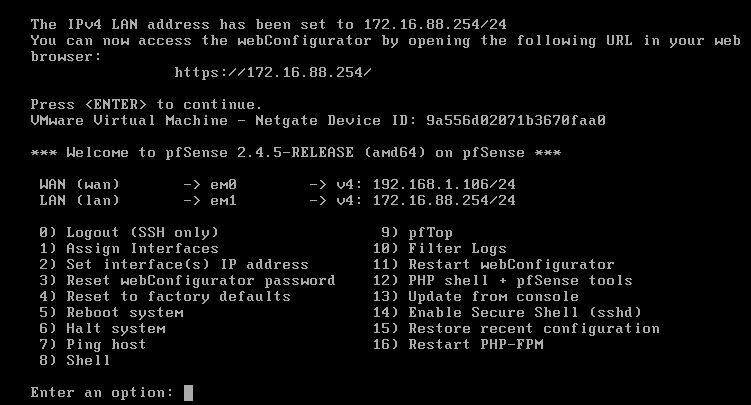
Set IP address cho các Interfaces:

WAN

LAN

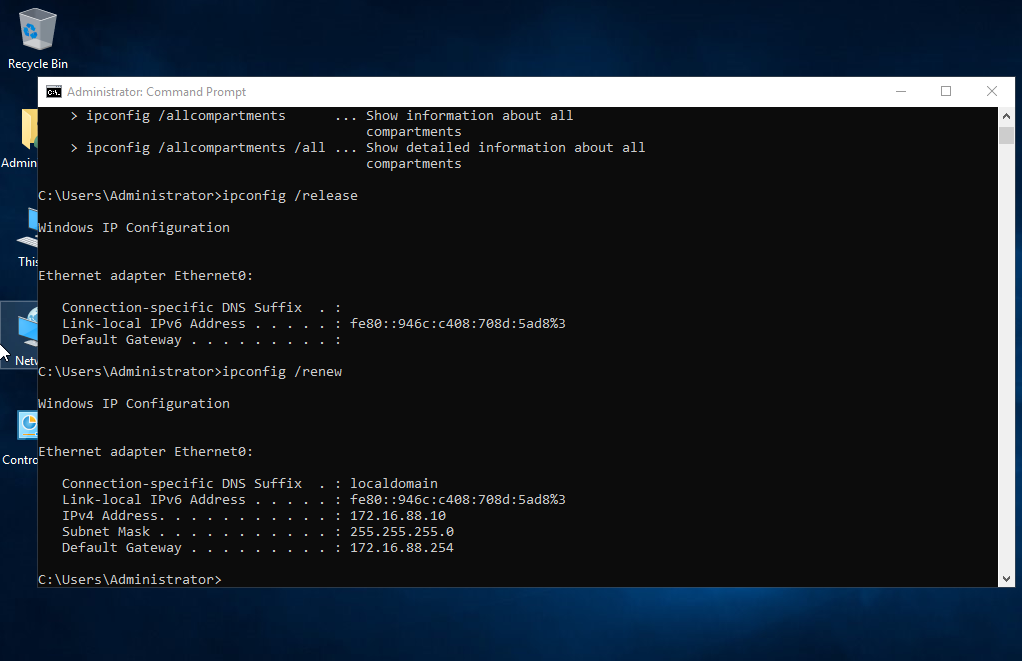


Sau khi cấu hình: WAN đã sử dụng cấu hình IP tĩnh

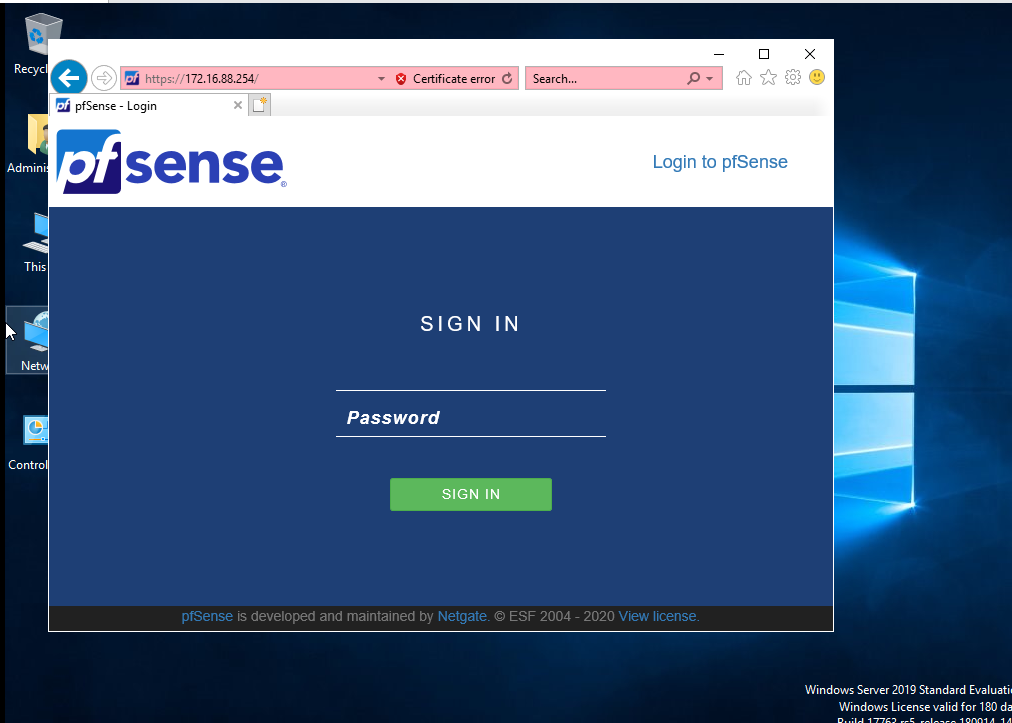


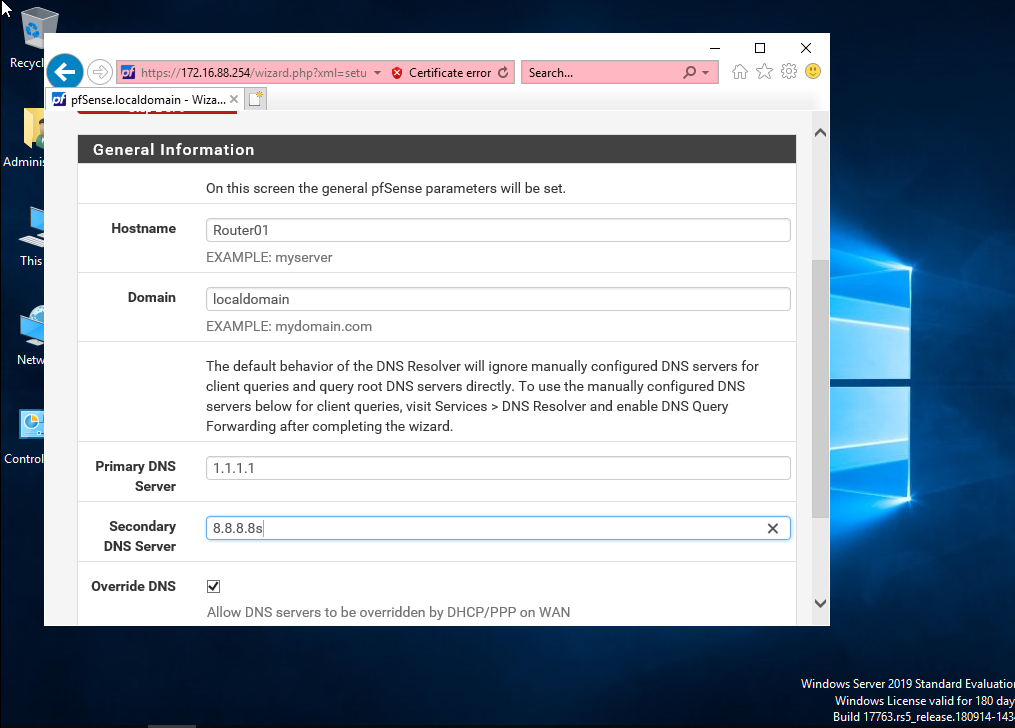
## 5.4 Cấu hình trên máy Window server

Renew ipconfig cho Window server

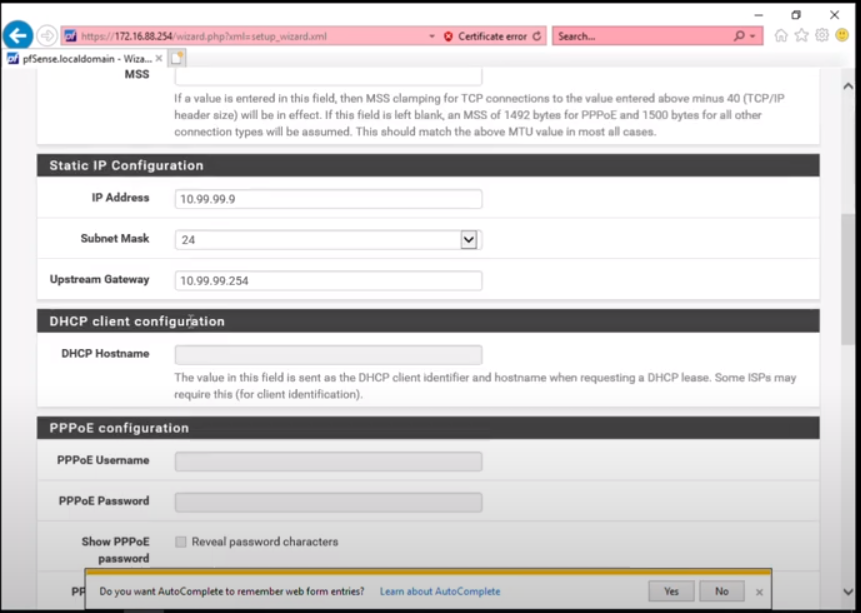


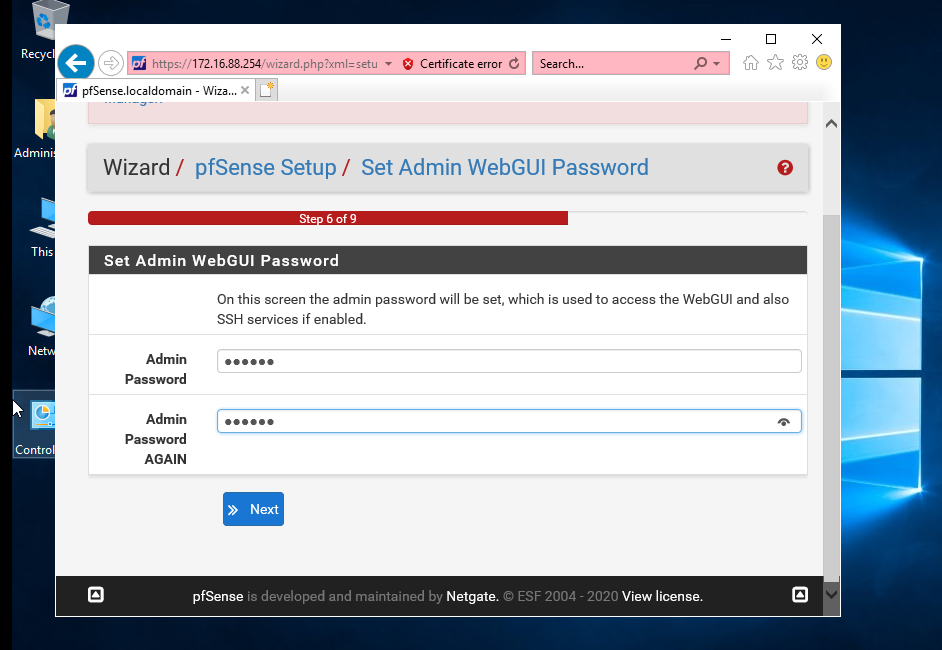
Truy cập địa chỉ PfSense



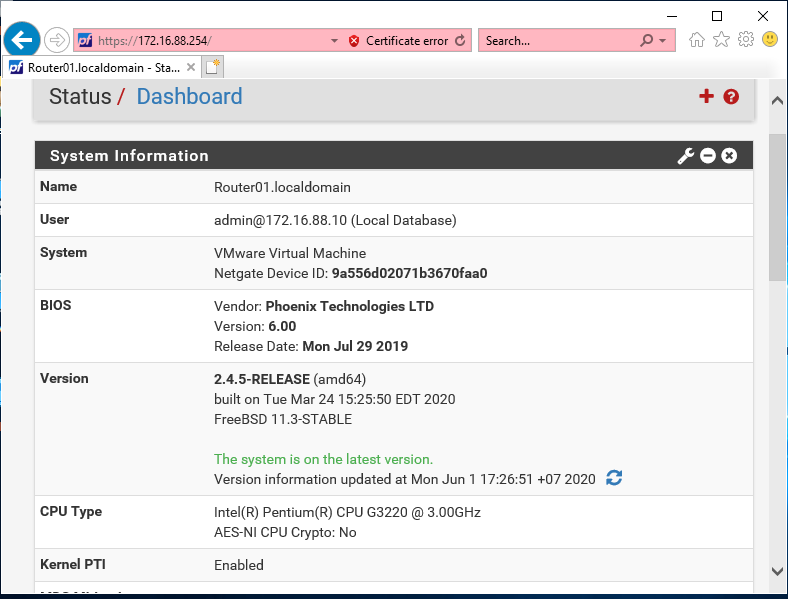


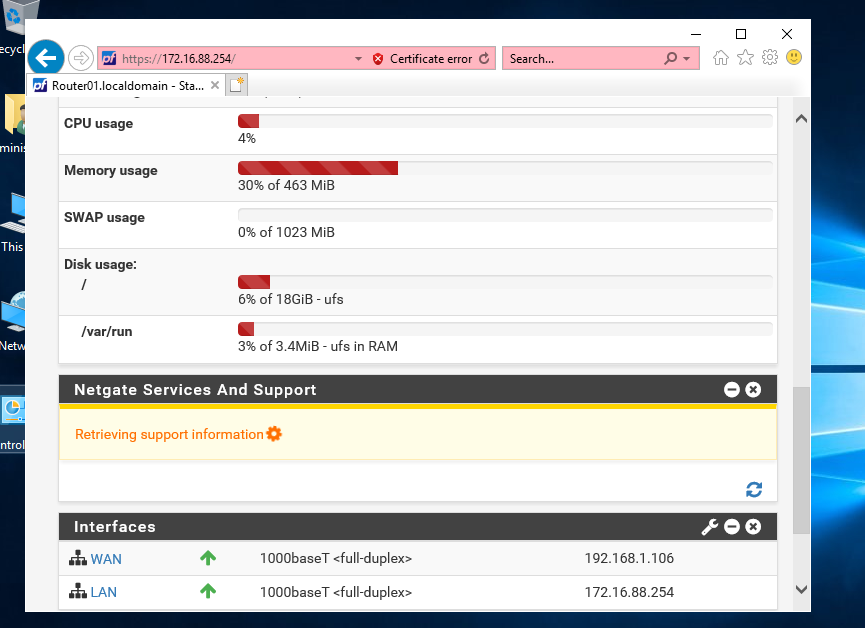






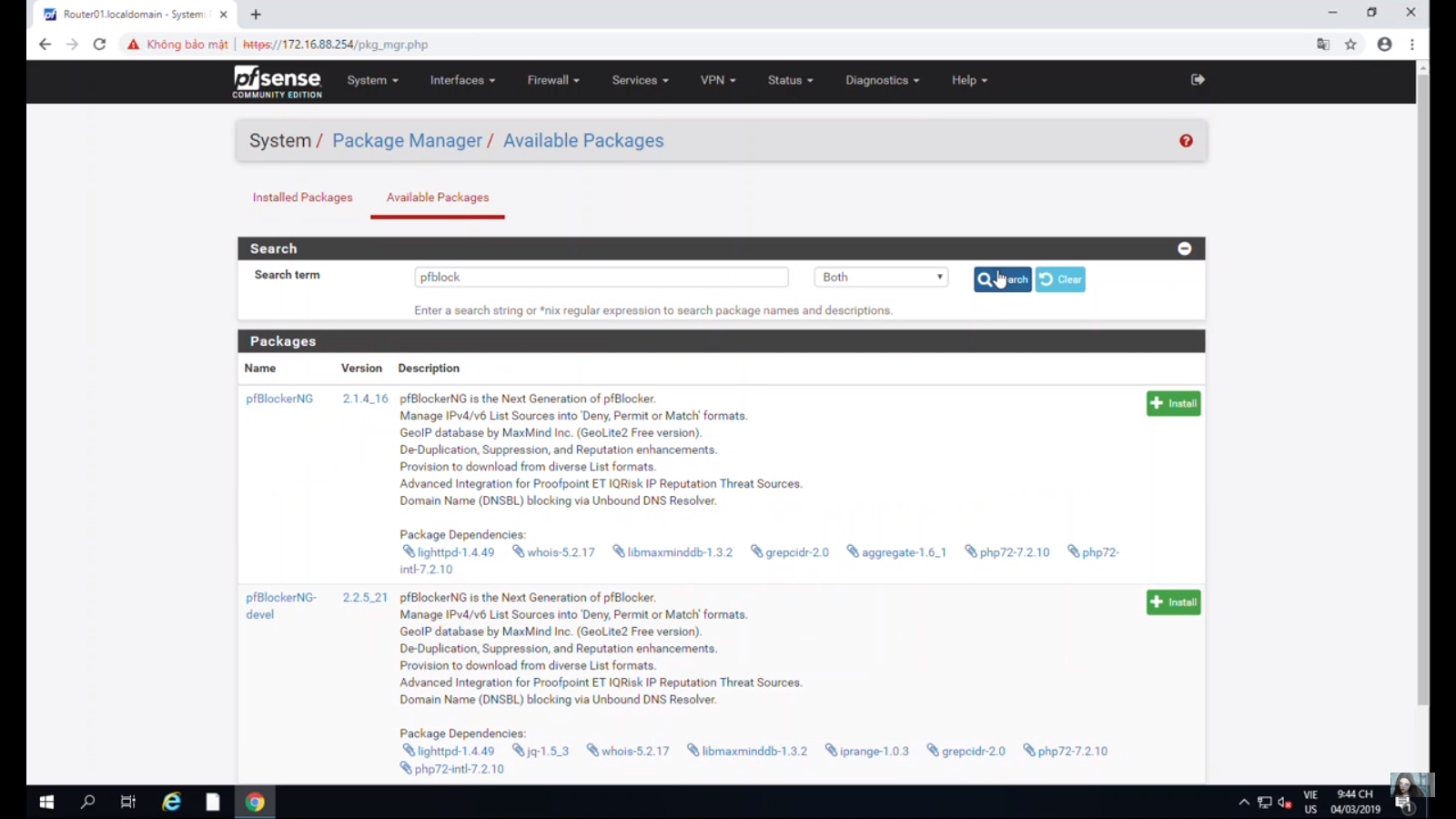
Cấu hình thành công

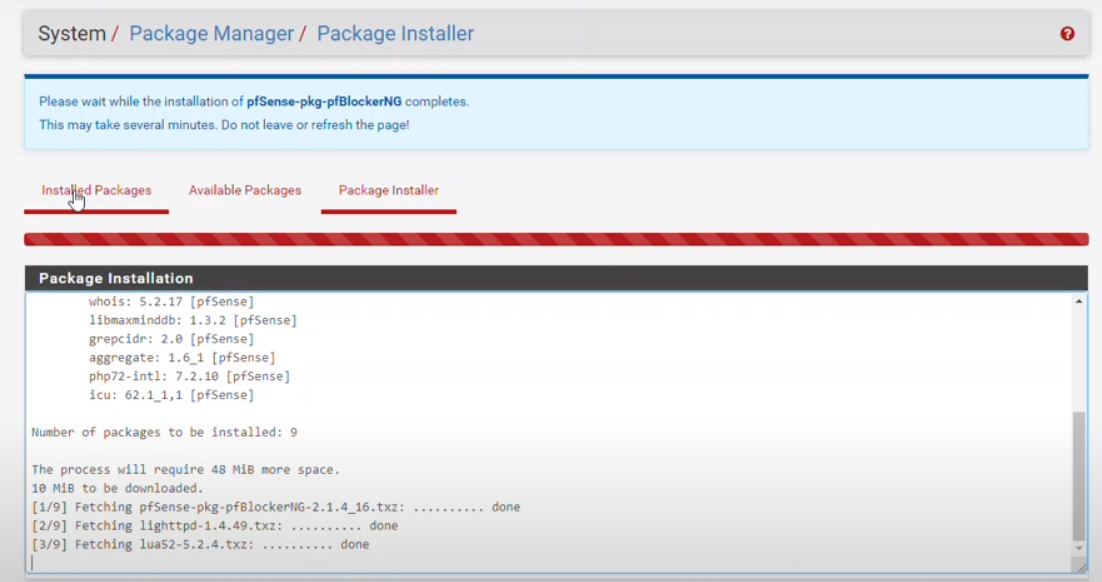




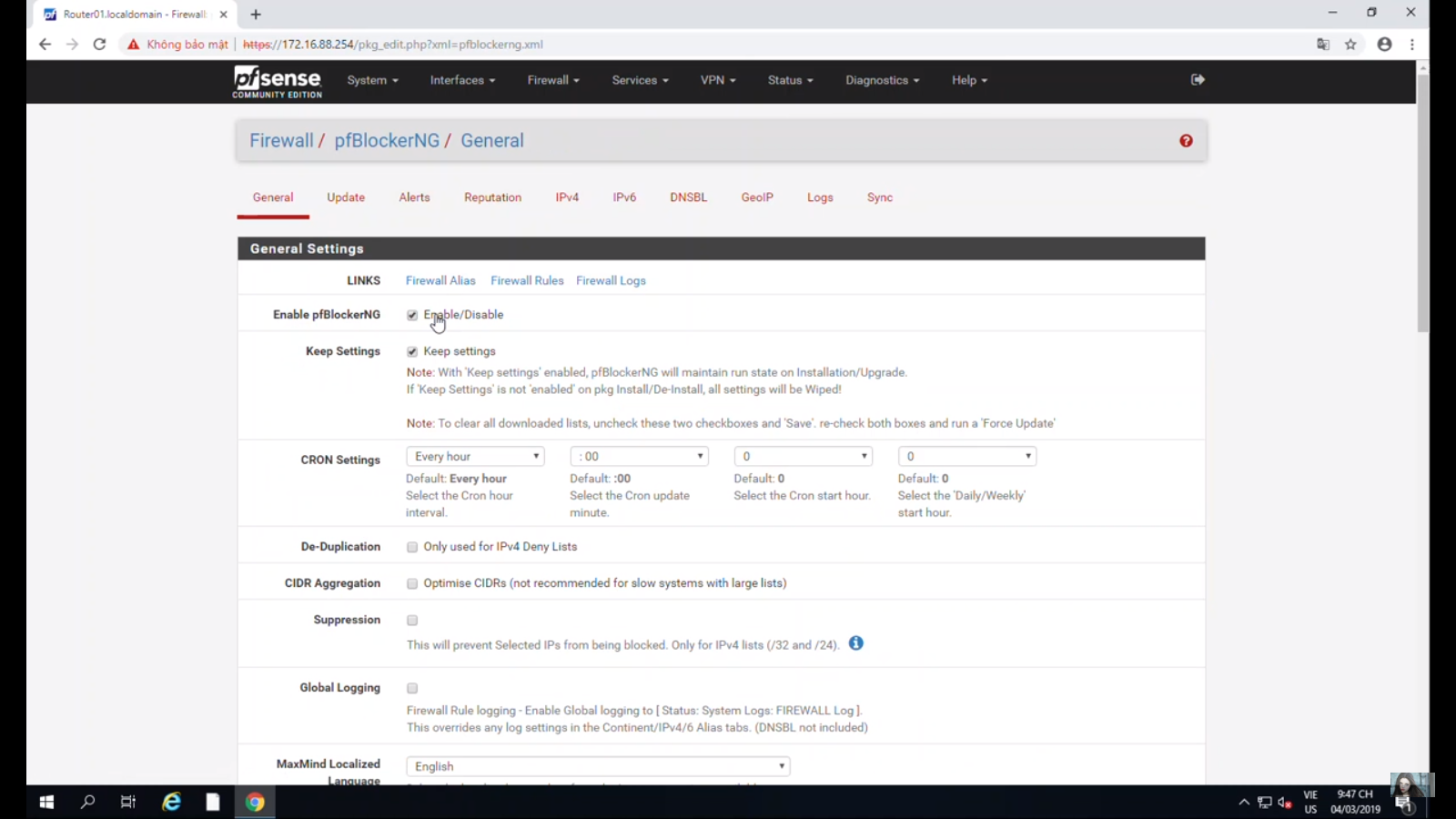
## 5.5 Chặn web và quảng cáo bằng PfSense

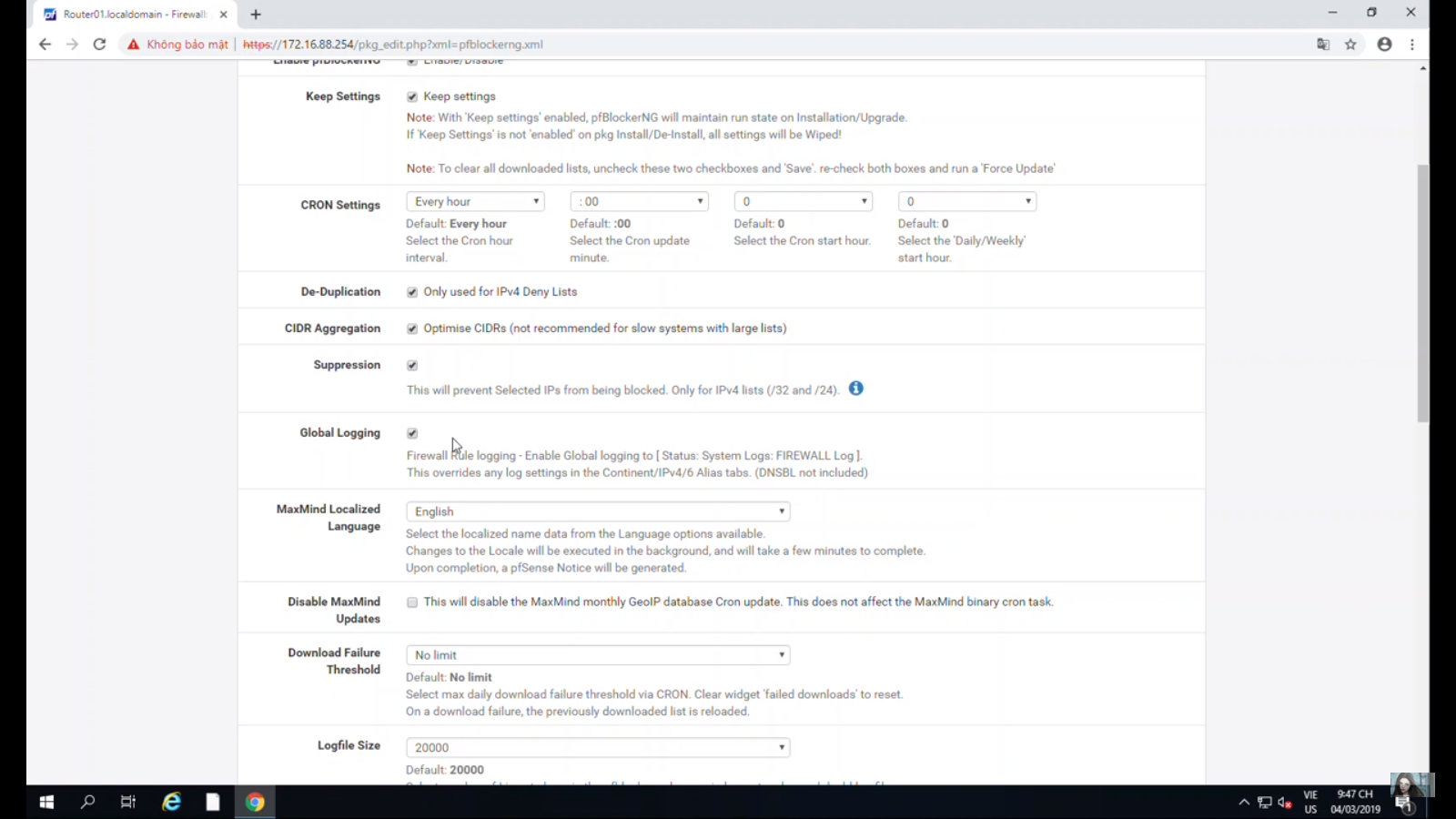
Cài đặt pfBlockerNG

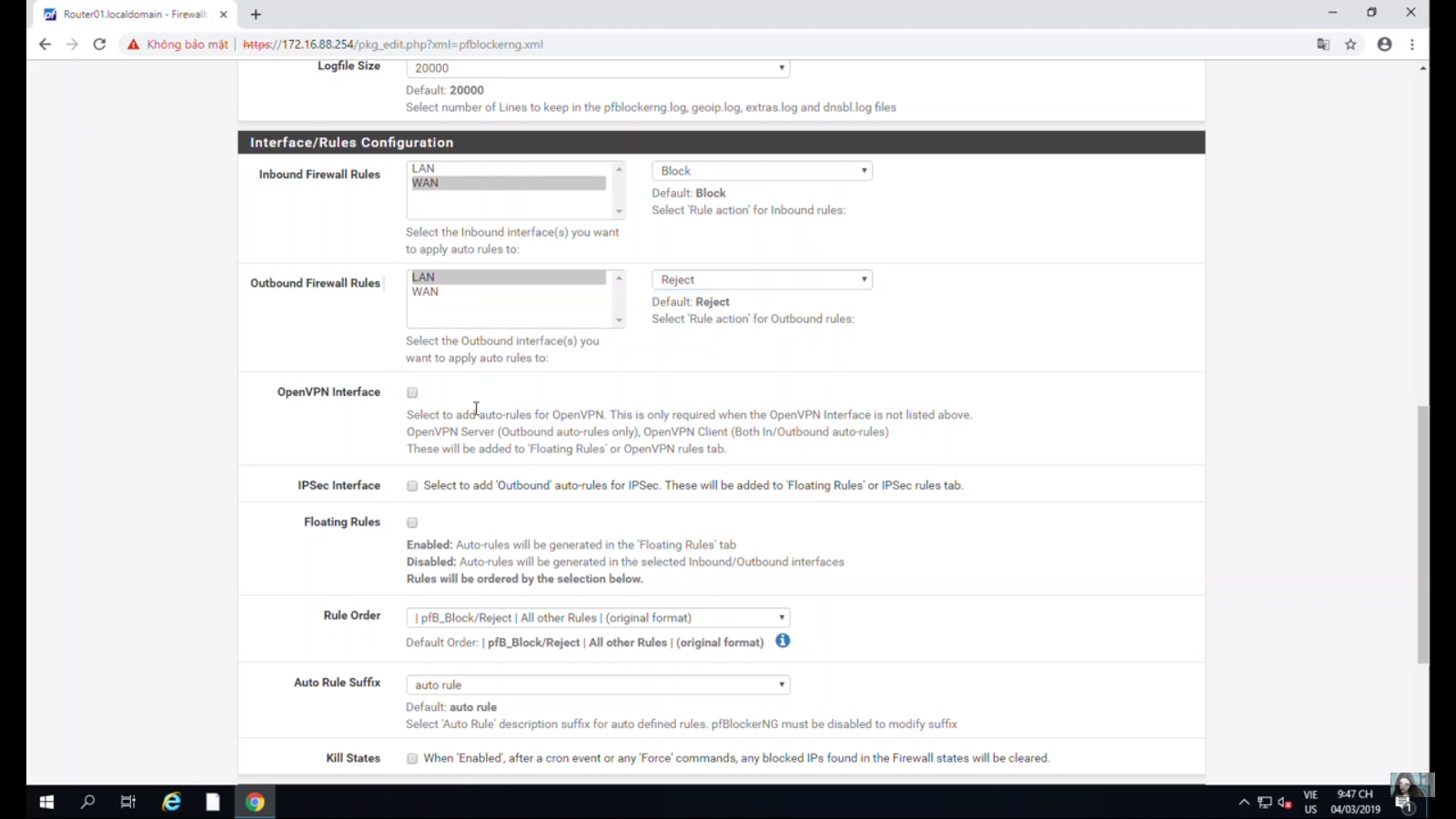




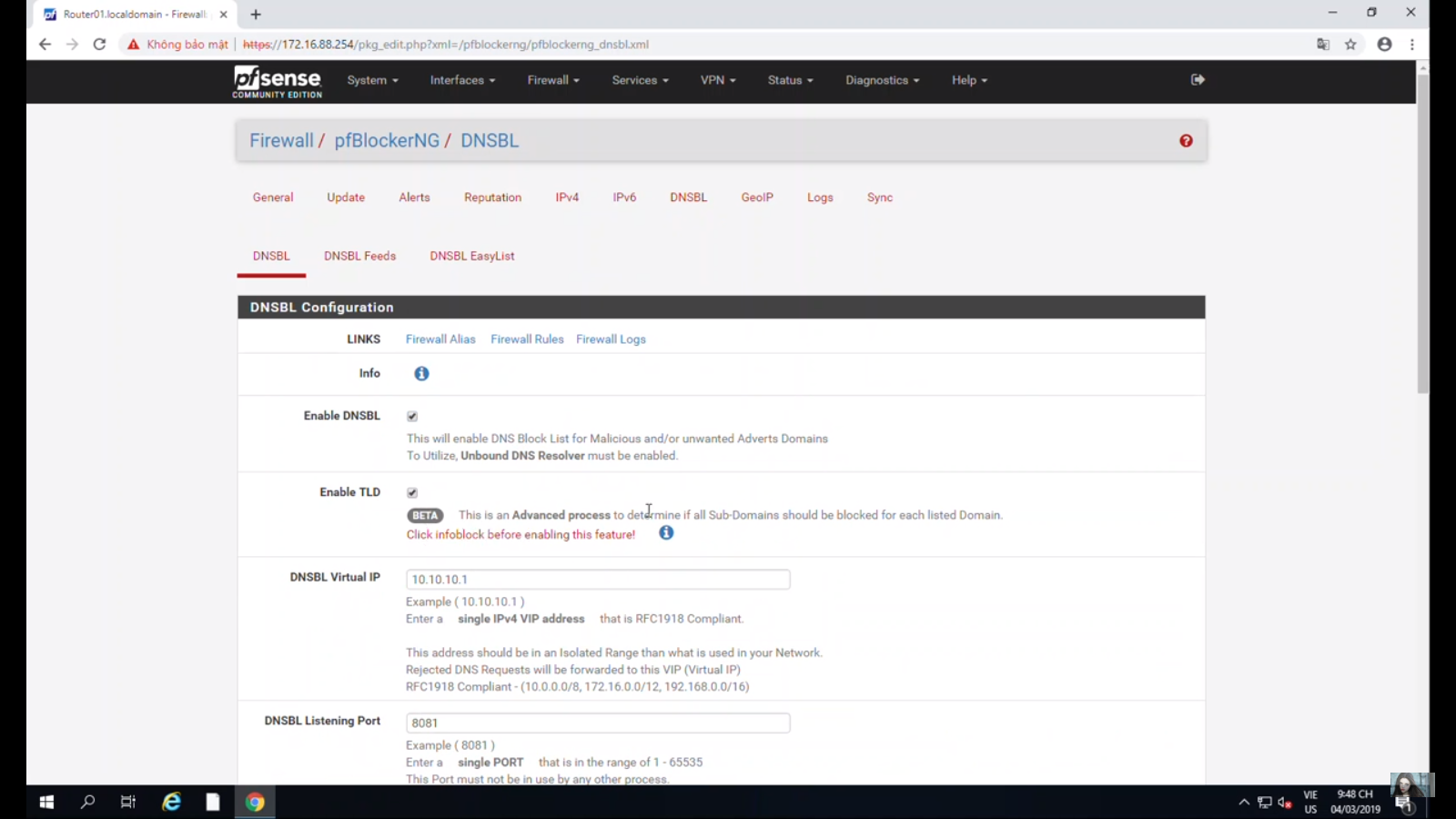
Sau khi cài đặt thành công, vào Firewall -> pfBlockerNG -> Enable



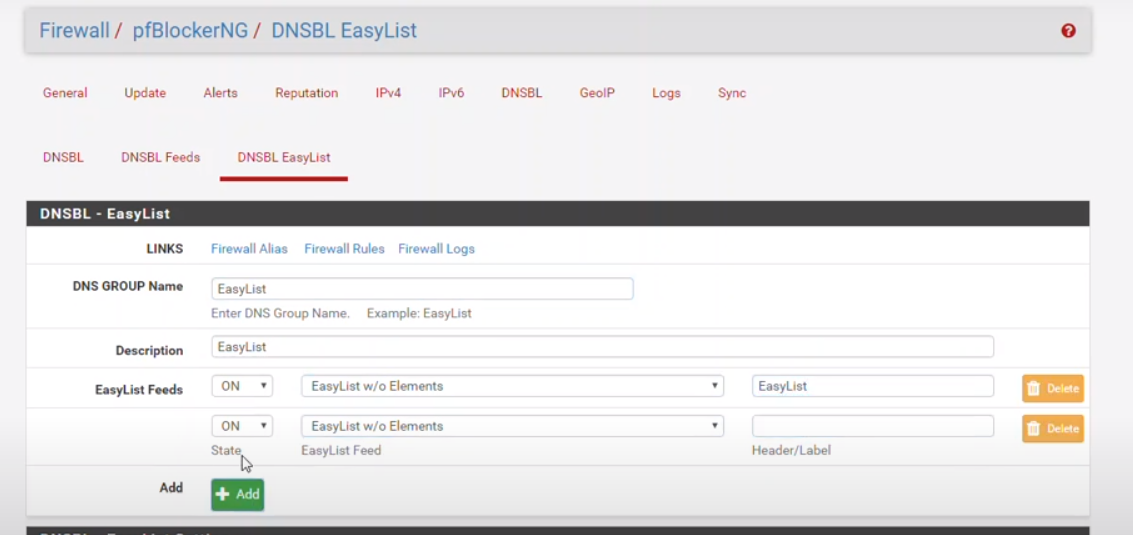




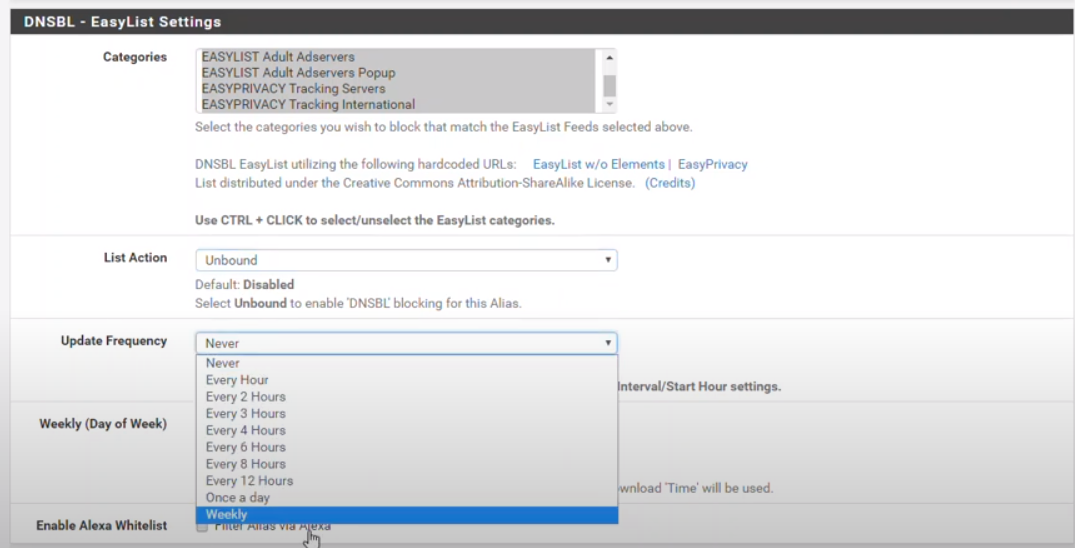
Vào DNSBL



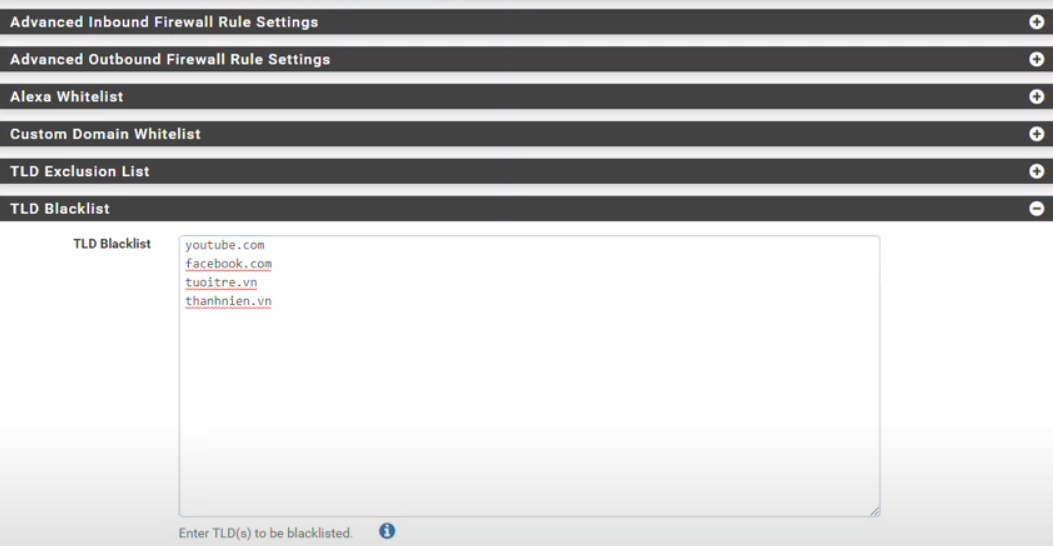
Để chặn quảng cáo, vào DNSBL EasyList

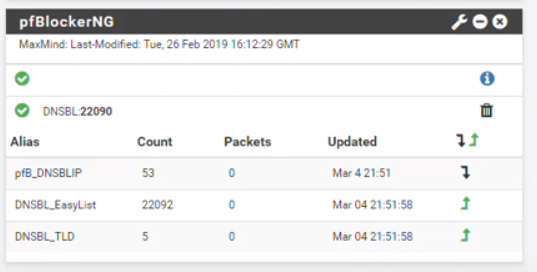


Tạo list, chặn hết các loại quảng cáo



Ds các page chặn





Kết quả

