BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN TỐT NGHIỆP**

**NGHIÊN CỨU CÀI ĐẶT TƯỜNG LỬA IPFire VÀ SO SÁNH VỚI PFsense**

**Giảng viên hướng dẫn: ThS. Cấn Thị Phượng**

**Sinh viên thực hiện: Nguyễn Đặng Trọng Thái**

**Mã số sinh viên: 61131036**

Khánh Hòa – 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN TỐT NGHIỆP**

**NGHIÊN CỨU CÀI ĐẶT TƯỞNG LỬA IPFire VÀ SO SÁNH VỚI PFsense**

GVHD: ThS. Cấn Thị Phượng

SVTH: Nguyễn Đặng Trọng Thái

MSSV: 61131036

Khánh Hòa – Tháng 12/2021

# LỜI CẢM ƠN

Để hoàn thành đề tài tốt nghiệp này, trước hết em xin gửi đến quý thầy, cô Khoa Công nghệ Thông tin - Trường Đại học Nha Trang lời cảm ơn chân thành.

Em xin gửi đến cô Cấn Thị Phượng, người đã tận tình hướng dẫn, giúp đỡ em hoàn thành đề tài tốt nghiệp này lời cảm ơn sâu sắc nhất.

Trong quá trình nghiên cứu thực hiện đề tài, cũng như là trong quá trình làm bài báo cáo tốt nghiệp, khó tránh khỏi sai sót, rất mong các thầy, cô bỏ qua. Đồng thời do kiến thức cũng như kinh nghiệm thực tiễn của bản thân còn hạn chế nên đề tài, bài báo cáo tốt nghiệp này khó thể không tránh khỏi những thiếu sót, em rất mong nhận được ý kiến đóng góp từ quý thầy, cô để em học hỏi thêm được nhiều kinh nghiệm, cũng như kỹ năng cần thiết.

Em xin chân thành cảm ơn!

# TÓM TẮT ĐỒ ÁN

Với thời gian thực hiện đồ án còn hạn chế nên đề tài “**Nghiên cứu cài đặt tường lửa IPFire và so sánh với PFsense**” chỉ dừng ở mức tìm hiểu về việc cài đặt, cấu hình và thực hiện một bài kiểm thử độ bảo mật của hai tường lửa.

Mục đích của việc so sánh giữa hai tường lửa là nhằm giúp cho người dùng có thể dễ dàng biết được đâu là hệ thống tường lửa phù hợp với môi trường mình cần cài đặt, cho cái nhìn hệ thống tổng thể và toàn diện có thể hỗ trợ việc lựa chọn được tiến hành nhanh hơn, kết quả chắc chắn hơn, từ đó có thể dễ dàng đưa ra quyết định một cách hiệu quả hơn.

Do khả năng của bản thân còn hạn chế, các dữ kiện để so sánh giữa hai tường lửa vẫn chưa đầy đủ nên việc so sánh chưa đạt tới mức độ chắc chắn 100% . Rất mong nhận được sự thông cảm và đóng góp ý kiến từ Quý Thầy/Cô và các bạn.

# MỤC LỤC

[LỜI CẢM ƠN i](#_Toc92374793)

[TÓM TẮT ĐỒ ÁN ii](#_Toc92374794)

[MỤC LỤC iii](#_Toc92374795)

[DANH MỤC HÌNH VẼ iv](#_Toc92374796)

[DANH MỤC CÁC TỪ VIẾT TẮT v](#_Toc92374797)

[MỞ ĐẦU 1](#_Toc92374798)

[Chương 1. TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU 3](#_Toc92374799)

[1.1 CƠ SỞ LÝ THUYẾT 3](#_Toc92374800)

[1.1.1 Tổng quan về tường lửa 3](#_Toc92374801)

[1.1.1.1 Lịch sử ra đời của tường lửa 3](#_Toc92374802)

[1.1.1.2 Mục đích của tường lửa 4](#_Toc92374803)

[1.1.1.3 Chức năng của tường lửa 5](#_Toc92374804)

[1.1.2 Tổng quan về công nghệ ảo hóa VMware 6](#_Toc92374805)

[1.1.2.1 Lịch sử ra đời của VMware Workstation 6](#_Toc92374806)

[1.1.2.2 Mục đích của VMware Workstation 6](#_Toc92374807)

[1.1.2.3 Chức năng của VMware Workstation 7](#_Toc92374808)

[1.1.3 Tổng quan về Kali Linux 8](#_Toc92374809)

[1.1.3.1 Lịch sử ra đời của Kali Linux 8](#_Toc92374810)

[1.1.3.2 Mục đích của Kali Linux 8](#_Toc92374811)

[1.1.3.3 Chức năng của Kali Linux 8](#_Toc92374812)

[1.2 CÁC BƯỚC KIỂM THỬ LỖ HỔNG BẢO MẬT 8](#_Toc92374813)

[1.2.1 Xác định vị trí tường lửa 8](#_Toc92374814)

[1.2.2 Tiến hành theo dõi - Traceroute 8](#_Toc92374815)

[1.2.3 Quét cổng 8](#_Toc92374816)

[1.2.4 Xác định phiên bản tường lửa 8](#_Toc92374817)

[1.2.5 Liệt kê danh sách truy cập 9](#_Toc92374818)

[1.2.6 Xác định kiến trúc tường lửa 9](#_Toc92374819)

[1.2.7 Kiểm tra chính sách tường lửa 9](#_Toc92374820)

[1.2.8 Lập bản đồ các thiết bị phía sau tường lửa – Firewalking 9](#_Toc92374821)

[1.2.9 Chuyển hướng cổng 9](#_Toc92374822)

[1.2.10 Kiểm tra bên ngoài và bên trong 9](#_Toc92374823)

[1.2.11 Kiểm tra kênh bí mật 9](#_Toc92374824)

[1.2.12 HTTP Tunneling 9](#_Toc92374825)

[1.2.13 Ghi chép và báo cáo 9](#_Toc92374826)

[1.3 THỰC TIỄN VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI 9](#_Toc92374827)

[1.4 TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU 9](#_Toc92374828)

[1.4.1 Tình hình nghiên cứu trên thế giới 9](#_Toc92374829)

[1.4.2 Tình hình nghiên cứu trong nước 10](#_Toc92374830)

[Chương 2. TỔNG QUAN VỀ TƯỜNG LỬA IPFire 11](#_Toc92374831)

[2.1 TƯỜNG LỬA IPFire 11](#_Toc92374832)

[2.2 NHỮNG CHỨC NĂNG CHÍNH CỦA TƯỜNG LỬA IPFire 11](#_Toc92374833)

[Chương 3. CẤU HÌNH VÀ CÀI ĐẶT TƯỜNG LỬA IPFire, PFsense 12](#_Toc92374834)

[3.1 HƯỚNG DẪN CÀI ĐẶT PHẦN MỀM HỖ TRỢ ẢO HÓA VMware 12](#_Toc92374835)

[3.2 HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA IPFire 12](#_Toc92374836)

[3.2.1 Hướng dẫn cài đặt tường lửa IPFire 12](#_Toc92374837)

[3.2.2 Hướng dẫn cấu hình tường lửa IPFire 17](#_Toc92374838)

[3.3 HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA PFsense 18](#_Toc92374839)

[3.3.1 Hướng dẫn cài đặt tường lửa PFsense 18](#_Toc92374840)

[3.3.2 Hướng dẫn cấu hình tường lửa PFsense 19](#_Toc92374841)

[Chương 4. THỰC HIỆN BÀI KIỂM TRA VỀ ĐỘ BẢO MẬT 19](#_Toc92374842)

[4.1 HƯỚNG DẪN CÀI ĐẶT Kali Linux 19](#_Toc92374843)

[4.2 THỰC HIỆN KIỂM THỬ LỖ HỔNG BẢO MẬT 19](#_Toc92374844)

[4.2.1 Kiểm thử lỗ hổng bảo mật trên IPFire 19](#_Toc92374845)

[4.2.2 Kiểm thử lỗ hổng bảo mật trên PFsense 19](#_Toc92374846)

[Chương 5. KẾT QUẢ 20](#_Toc92374847)

[5.1 KẾT QUẢ ĐẠT ĐƯỢC 20](#_Toc92374848)

[5.2 ƯU ĐIỂM CỦA TƯỜNG LỬA IPFire 20](#_Toc92374849)

[5.3 HẠN CHẾ CỦA TƯỜNG LỬA IPFire 20](#_Toc92374850)

[5.4 KẾT LUẬN 20](#_Toc92374851)

[TÀI LIỆU THAM KHẢO 20](#_Toc92374852)

[PHỤ LỤC 20](#_Toc92374853)

[1. Phụ lục 1: 20](#_Toc92374854)

# DANH MỤC HÌNH VẼ

# DANH MỤC CÁC TỪ VIẾT TẮT

# MỞ ĐẦU

* **Lý do chọn đề tài:**

Tường lửa là một thiết bị bảo mật giám sát lưu lượng mạng. Nó bảo vệ mạng nội bộ bằng cách lọc lưu lượng đến và đi dựa trên một tập hợp các quy tắc đã thiết lập. Thiết lập tường lửa là cách đơn giản nhất để thêm một lớp bảo mật giữa hệ thống và các cuộc tấn công độc hại.

Tường lửa là một yêu cầu đối với các tổ chức cấp doanh nghiệp và được khuyến nghị trong bất kỳ môi trường mạng nào.

Mặc dù tất cả đều phục vụ để ngăn chặn truy cập trái phép, nhưng các phương pháp hoạt động và cấu trúc tổng thể của tường lửa có thể khá đa dạng. Theo cấu trúc của chúng, có ba loại tường lửa – tường lửa phần mềm, tường lửa phần cứng hoặc cả hai.

Trong một số trường hợp, việc mua tường lửa cứng có thể nằm ngoại phạm vi ngân sách của tổ chức. Trong trường hợp này, tùy thuộc vào lưu lượng truy cập dự kiến đi qua mạng, một máy tính để bàn không sử dụng tới có thể trở thành tường lửa phần cứng, điều này có thể được thực hiện với hệ điều hành tường lửa dựa trên hệ thống Linux.

Hiện nay có nhiều yếu tổ ảnh hưởng tới việc lựa chọn tường lửa tốt nhất, và đó là một vấn đề lớn.

Vì những lí do trên, nên em đã chọn đề tài: **“Nghiên cứu và cài đặt tường lửa IPFire và so sánh với PFsense**” làm đề tài tốt nghiệp của mình.

* **Mục tiêu nghiên cứu:**
* ***Mục tiêu chung:*** Nghiên cứu, cài đặt tường lửa IPFire và so sánh với PFsense dựa trên Kali Linux để thực hiện các quy trình kiểm thử, tấn công. Từ đó đưa ra những nhận định khách quan nhất giữa hai tường lửa.
* ***Mục tiêu cụ thể:***
* Tìm hiểu tưởng lửa IPFire và PFsense.
* Thực hiện các quy trình kiểm thử.
* Nhận định và so sánh giữa hai tường lửa.
* **Nội dung và phương thức thực hiện:**
* ***Nội dung thực hiện:***
* Khảo sát các đánh giá của người dùng tưởng lửa IPFire và PFsense.
* Tìm hiểu tưởng lửa IPFire và PFsense.
* Cài đặt và cấu hình tưởng lửa IPFire và PFsense trên môi trường máy ảo VMware Workstation.
* Thực hiện các quy trình kiểm thử dựa trên Kali Linux.
* Nhận định và so sánh giữa hai tường lửa dựa trên các dữ kiện đã thu nhập.
* ***Phương pháp:***
* ….
* **Cấu trúc của báo cáo bao gồm:**

**Chương 1:** Cơ sở lý thuyết.

**Chương 2:** Tổng quan về tường lửa IPFire.

**Chương 3:** Cấu hình và cài đặt tưởng lửa IPFire, PFsense.

**Chương 4:** Thực hiện bài kiểm tra về độ bảo mật.

**Chương 5:** Những kết quả, ưu điểm và mặt hạn chế giữa hai tường lửa.

# TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU

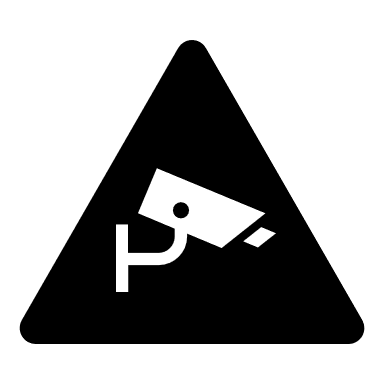
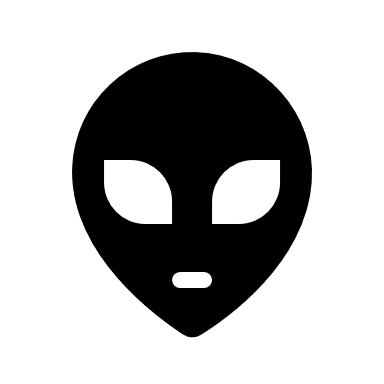
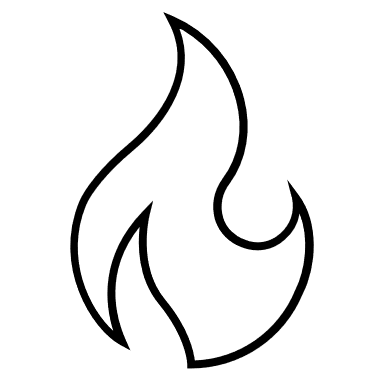
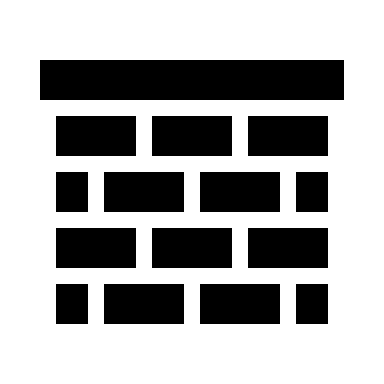
## CƠ SỞ LÝ THUYẾT

### Tổng quan về tường lửa

#### Lịch sử ra đời của tường lửa

Trong lĩnh vực mạng máy tính, tường lửa (Firewall) là một kỹ thuật trong hệ thống mạng để chống lại sự truy cập trái phép, tường lửa ra đời nhằm mục đích bảo vệ thông tin nội bộ trong một môi trường và hạn chế sự xâm nhập trái phép vào hệ thống, tường lửa có thể được coi rằng nó là một cơ chế bảo vệ mạng tin cậy khỏi các trang mạng không tin cậy.

Thông thường, tường lửa sẽ được đặt giữa mạng nội bộ của một môi trường và Internet. Nó đảm bảo vai trò chính là bảo mật thông tin, ngăn chặn sự truy cập không mong muốn từ Internet vào và cấm truy cập từ bên trong ra một số địa chỉ nhất định trên Internet.

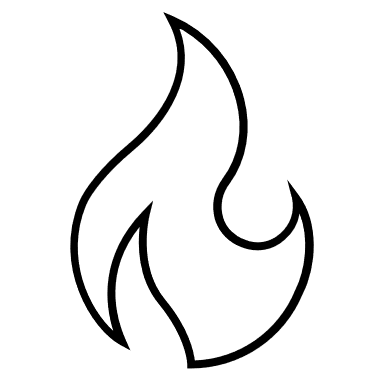
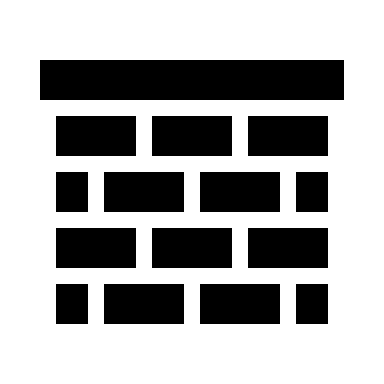


Mạng nội bộ (LAN)

Mạng diện rộng (WAN)

Hình 1.1.1.1.1 Sơ đồ hoạt động của tường lửa

Ngoài ra, trong một số trường hợp thì tường lửa cũng có thể được thiết lập trong cùng một mạng nội bộ hoặc cô lập trong một khu vực nhất định. Ví dụ như một công ty sử dụng tường lửa để ngăn cách phòng họp nội bộ và showroom bán hàng ở tầng dưới.



Mạng nội bộ tầng 2



Mạng nội bộ tầng 1

Mạng nội bộ công ty

Hình 1.1.1.1.2 Sơ đồ hoạt động của tường lửa trong môi trường mạng nội bộ

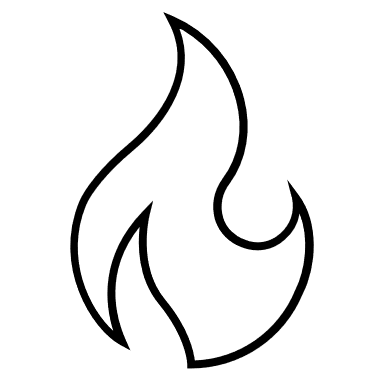
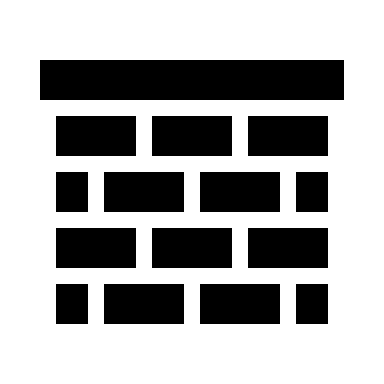
Tường lửa hoạt động theo cách kiểm tra thông tin vào và ra Internet. Nó nhận dạng và từ chối truy cập các thông tin tới tự những địa chỉ nguy hiểm hoặc có vẻ nghi ngờ. Tường lửa là một giải pháp dựa trên phần cứng hoặc phần mềm dùng để kiểm tra các thông tin. Tường lửa là một giải pháp cần phải có cho bất kỳ máy tính nào có kết nối Internet nhất là những loại kết nối luôn luôn trong trạng thái hoạt động như kết nối Internet băng thông rộng, đây là loại kết nối thuận lợi cho những tin tặc sử dụng làm phương tiện tấn công vào các máy tính khác.

#### Mục đích của tường lửa

Tường lửa ra đời nhằm mục đích có thể được xem như một người gác cổng có nhiệm vụ kiểm tra “giấy thông hành” của các gói tin ra vào của máy tính, chỉ cho phép các gói tin hợp lệ được đi qua. Tường lửa sẽ đảm bảo tất cả các dữ liệu đi vào là hợp lệ, ngăn chặn những tin tặc cố ý làm cho các gói dữ liệu lắp ghép sai thứ tự sau khi quá trình phân mảnh IP được tiến hành để gửi dữ liệu vào máy tính người dùng nhằm mục đích nắm quyền kiểm soát trái phép. Đây là chức năng rất quan trọng của tường lửa vì nó sẽ giúp máy tính tránh được những tin tặc cài virus, mã độc,… vào máy tính.

Một tường lửa gồm tối thiểu hai giao diện mạng: Giao diện mạng chung được kết nối với Internet cho phép mọi người có thể truy cập. Giao diện mạng riêng là nơi chứa các dữ liệu được bảo vệ. Trên một hệ thống tường lửa có thể có nhiều giao diện riêng tùy vào số phân đoạn mạng nội bộ và giao diện có những quy tắc bảo vệ riêng. Việc thiết lập phân đoạn mạng giúp cho các nhà quản trị mạng tăng khả năng bảo mật vì tường lửa là lớp bảo vệ sau của bộ định tuyến, ở đây cho thấy tường lửa rất hữu ích bởi vì bộ định tuyến thường làm việc quá tải. Vì vậy các nhà quản trị mạng sẽ thường sử dụng hai lớp tường lửa, lớp thứ nhất để bảo vệ toàn bộ hệ thống mạng, lớp thứ hai sẽ bảo vệ những phân đoạn mạng. Việc này cho phép ta kiểm soát dữ liệu tốt hơn, các hoạt động vào ra của dữ liệu có thể được cho phép trên một đoạn mạng nhất định nhưng sẽ bị giới hạn ở đoạn nhạy cảm hơn.

Hình 1.1.1.2 Sơ đồ thiết lập 2 Tường lửa cho mạng nội bộ có phân đoạn mạng



Ban kiểm toán

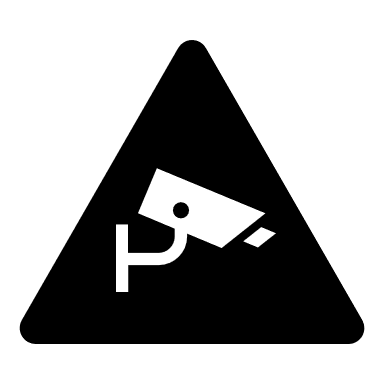
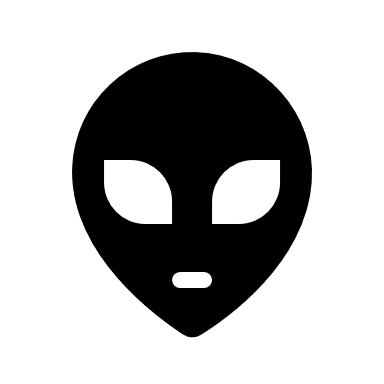
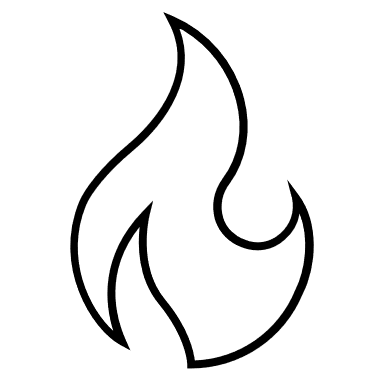
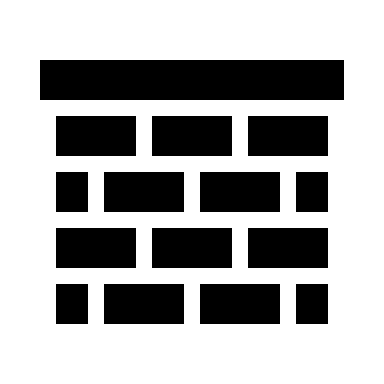


Ban sản xuất

Mạng nội bộ công ty



Ban quản trị



Mạng diện rộng (WAN)

Tường lửa bảo vệ mạng từ những lưu lượng không mong muốn. Một tường lửa có thể được cấu hình để chặn tất cả các lưu lượng mạng ngoài trừ cổng 53 của máy chủ DNS.

#### Chức năng của tường lửa

Tường lửa giúp bảo vệ được những dữ liệu, tài nguyên của hệ thống. Một số chức năng của tường lửa là có thể bảo mật được những thông tin quan trọng trong môi trường mạng tin cậy, bảo đảm tính toàn vẹn và kịp thời của thông tin.

Tường lửa chống lại những sự tấn công từ môi trường mạng không tin cậy và môi trường Internet.

- Ngăn chặn Hacking.

- Ngăn chặn việc thay đổi mã.

- Từ chối dịch vụ.

- Ngăn chặn tấn công trực tiếp (Dò mật khẩu, sử dụng lỗi của phần mềm).

- Ngăn chặn nghe trộm.

- Ngăn chặn Deny Service.

- Ngăn chặn sai sót từ người dùng, người quản trị.

### Tổng quan về công nghệ ảo hóa VMware

#### Lịch sử ra đời của VMware Workstation

VMWare Workstation là một hypervisor (phần mềm máy ảo) chạy trên hệ điều hành Windows và Linux cho phép người dùng thiết lập một hoặc nhiều máy ảo trên một máy vật lý và sử dụng đồng thời cùng với máy vật lý. Mỗi máy ảo có thể thực hiện hệ điều hành của riêng mình. VMWare Workstation hỗ trợ các bộ điều hợp mạng máy chủ hiện có và chia sẻ ổ đĩa vật lý với máy ảo. Nó cho phép tệp tin ISO có thể được gắn dưới dạng ổ đĩa ảo và được triển khai dưới dạng tệp .vmdk

#### Mục đích của VMware Workstation

VMWare Workstation ra đời nhằm phục vụ người dùng khắc phục một số hạn chế khi sử dụng chỉ một máy tính duy nhất. Vì mỗi máy ảo có thể thiết lập một địa chỉ IP khác nhau nên việc sử dụng VMWare Workstation có thể giúp người dùng chạy và làm việc độc lập với máy tính vật lý, nó giúp người dùng dùng thử một hệ điều hành mới, chạy cùng lúc nhiều phần mềm dành riêng cho các hệ điều hành khác nhau trên máy tính, các lập trình viên sau khi tạo ra một phần mềm họ sẽ có thể kiểm tra hoạt động của phần mềm đó trên tất cả các hệ điều hành trước khi phát hành tới tay người sử dụng, ngoài ra người dùng có thể truy cập các trang web có độ an toàn thấp, nếu bị nhiễm virus hoặc hư hỏng nó có thể được loại bỏ và thay thế bằng một bản sao mới hoàn toàn một cách nhanh chóng.

#### Chức năng của VMware Workstation

Một số tính năng của VMWare Workstation được thiết lập nhằm đáp ứng nhu cầu sử dụng đa dạng của người dùng.

-Giao diện gọn gàng và đơn giản. Tốc độ đồ họa cao giúp người dùng có thể chạy các ứng dụng đồ họa nặng trên máy ảo mà không gặp bất kỳ sự cố nào. Hơn nữa chương trình còn được tích hợp thư viện máy ảo, cho phép người dùng tìm kiếm và truy cập hệ điều hành khác một cách nhanh chóng. Ngoài ra, nó hỗ trợ độ phân giải QHD và 4K UHD để hiển thị tốt hơn.

-Đa dạng hệ điều hành. Phần mềm này tạo ra một lớp ảo hóa giữa hệ điều hành chủ và hệ điều hành ảo. Điều này cho phép người dùng Windows hoặc Linux chạy đồng thời nhiều hệ điều hành như macOS, Linux, Android, Windows trên thiết bị.

-Thiết lập môi trường bảo mật. Chương trình này cho phép người dùng chạy hệ thống thứ hai với độ bảo mật cao nhất. Người dùng có thể sử dụng chương trình để chạy một hệ điều hành có các cài đặt về quyền riêng tư, công cụ và cấu hình mạng khác với desktop chính. Chương trình cũng cung cấp một loạt các công cụ mà bạn có thể sử dụng để kiểm tra bất kỳ lỗ hổng nào trong máy ảo của mình.

-Hoàn tác snapshot. Chương trình cho phép người dùng chụp nhiều snapshot của hệ điều hành để nếu có gì sai sót, có thể hoàn tác về snapshot trước đó. Tất cả snapshot xuất hiện trong một hệ thống phân cấp phức tạp dạng cây và người dùng có thể quay lại một snapshot tùy ý bất cứ khi nào có nhu cầu. Hơn nữa, người dùng có thể tạo snapshot ngay cả khii máy ảo đang tắt hoặc bị treo.

-Kết nối với các server khác. Chương trình này cho phép người dùng kết nối an toàn với các server khác. Bằng cách này, người dùng có thể chỉnh sửa vai trò, thay đổi quyền, quản lý các hành động và tạo các máy ảo bổ sung,… Thông qua chức năng này, người dùng có thể quản lý các máy ảo từ xa như quản lý bất kỳ hệ điều hành khách nào trên máy tính vật lý.

-Chia sẻ máy ảo. Chương trình này hỗ trợ chia sẻ máy ảo với người dùng khác đang chạy cùng chương trình. Vì vậy nếu có kết nối Internet, người dùng có thể kết nối từ xa với các máy ảo khác. Chức năng này cho phép tạo ra một máy chủ mạnh mẽ và cho phép máy tính không có đủ tài nguyên kết nối và chạy nhiều hệ điều hành khác nhau.

-Chức năng mã hóa giúp người dùng có quyền truy cập vào một tính năng điều khiển cho phép mã hóa và thêm các hạn chế vào máy ảo. Mã hóa hệ điều hành ảo giúp ngăn chặn truy cập trái phép có thể dẫn đến vi phạm dữ liệu và chỉnh sửa cấu hình. Sau khi mã hóa máy ảo, cách duy nhất mọi người có thể truy cập nó là thông qua tên người dùng và mật khẩu.

### Tổng quan về Kali Linux

#### Lịch sử ra đời của Kali Linux

…

#### Mục đích của Kali Linux

…

#### Chức năng của Kali Linux

…

## CÁC BƯỚC KIỂM THỬ LỖ HỔNG BẢO MẬT

### Xác định vị trí tường lửa

…

### Tiến hành theo dõi - Traceroute

…

### Quét cổng

…

### Xác định phiên bản tường lửa

…

### Liệt kê danh sách truy cập

…

### Xác định kiến trúc tường lửa

…

### Kiểm tra chính sách tường lửa

…

### Lập bản đồ các thiết bị phía sau tường lửa – Firewalking

…

### Chuyển hướng cổng

…

### Kiểm tra bên ngoài và bên trong

…

### Kiểm tra kênh bí mật

…

### HTTP Tunneling

…

### Ghi chép và báo cáo

…

## THỰC TIỄN VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI

…

## TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU

### Tình hình nghiên cứu trên thế giới

…

### Tình hình nghiên cứu trong nước

…

# TỔNG QUAN VỀ TƯỜNG LỬA IPFire

## TƯỜNG LỬA IPFire

…

## NHỮNG CHỨC NĂNG CHÍNH CỦA TƯỜNG LỬA IPFire

…

# CẤU HÌNH VÀ CÀI ĐẶT TƯỜNG LỬA IPFire, PFsense

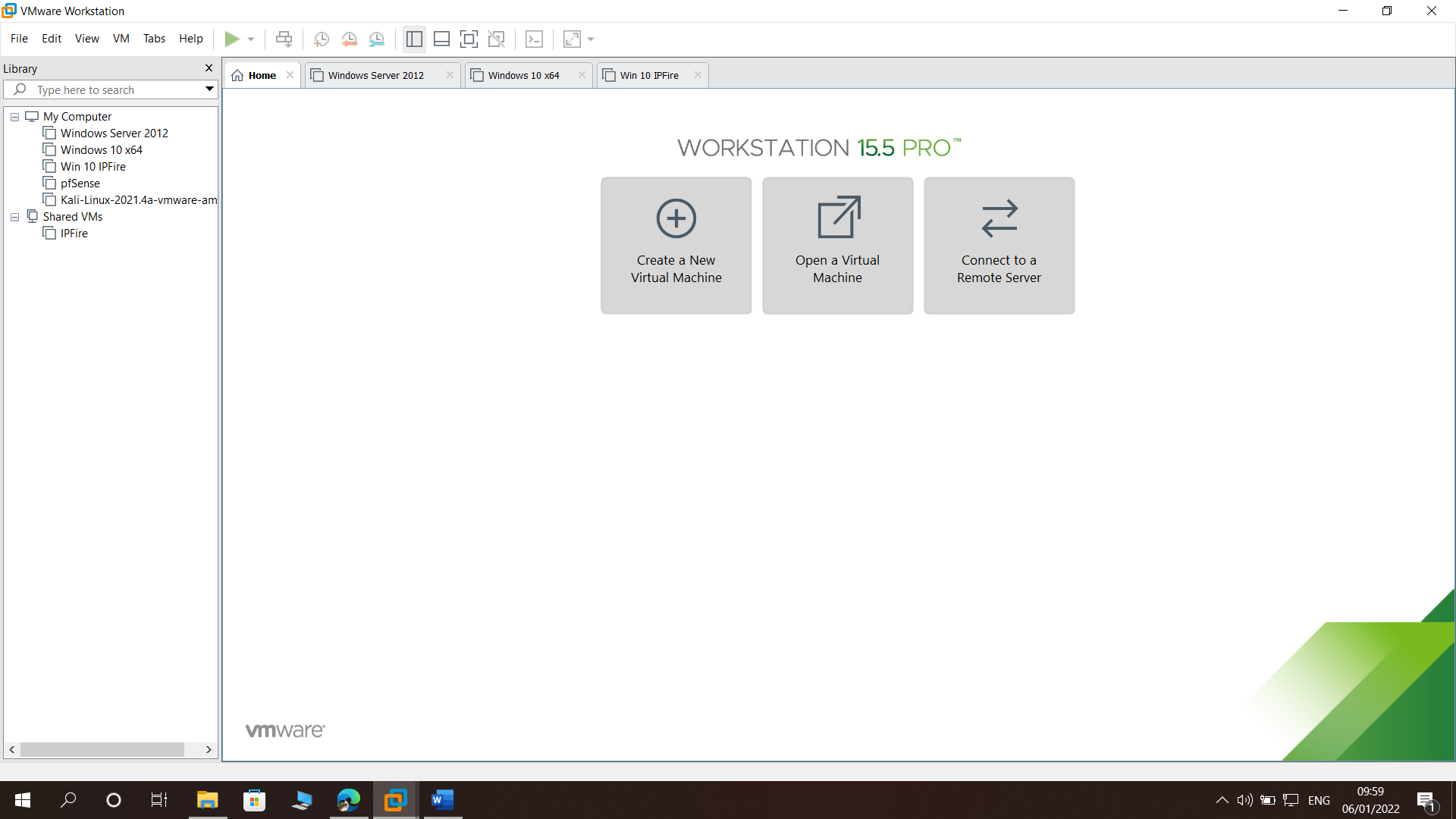
## HƯỚNG DẪN CÀI ĐẶT PHẦN MỀM HỖ TRỢ ẢO HÓA VMware

…

## HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA IPFire

### Hướng dẫn cài đặt tường lửa IPFire

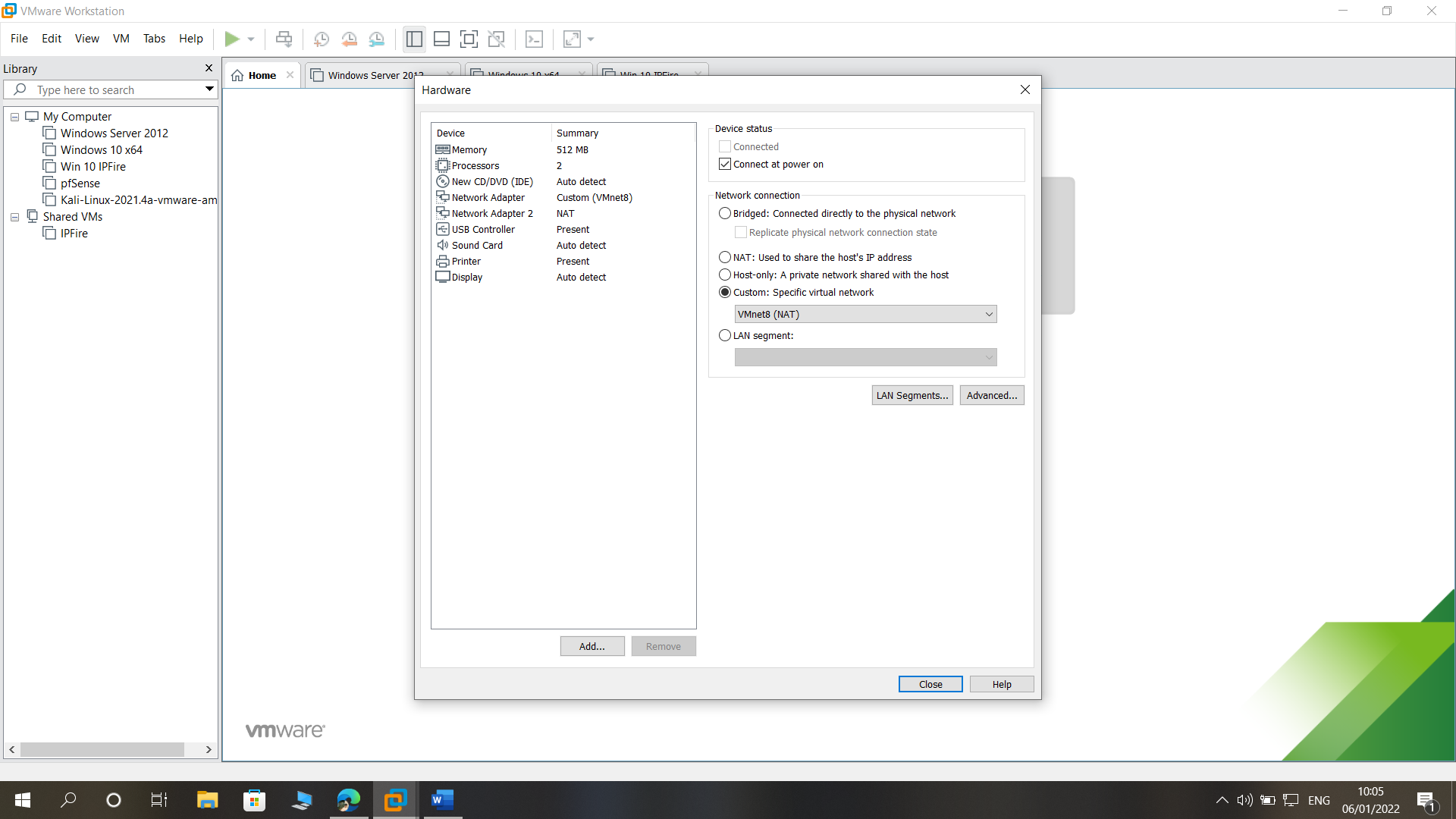
Download tường lửa IPFire từ trang chủ [www.ipfire.org](http://www.ipfire.org)

Sau khi download xong ta tiến hành cài đặt tường lửa IPFire trên phần mềm ảo hóa VMWare, tạo một máy ảo mới, chọn Create a New Virtual Machine trên giao diện chính của phần mềm.

Hình 3.2.1.1 Giao diện chính của phần mềm VMWare Workstation

Tại bước chọn hệ điều hành ta chọn hệ điều hành Linux.

Thiết lập cấu hình phần cứng cho máy ảo Linux này. Chọn CD/DVD sử dụng file ISO đã tải về từ trang chủ IPFire.

Hình 3.2.1.2 Thiết lập phần cứng cho máy ảo

Trong khuôn khổ bài báo cáo này, ta thiết lập 3 card mạng tương ứng 3 vùng

GREEN: (VMnet8 với IP 192.168.1.0) vùng mạng nội bộ có địa chỉ MAC: 00:0C:29:BF:B6:1F

RED: (VMnet9 lựa chọn Bridged và chọn card mạng vật lý của máy thật) vùng mạng Internet bên ngoài có địa chỉ MAC: 00:0C:29:BF:B6:15

ORANGE: (VMnet0) Vùng mạng DMZ có địa chỉ MAC: 00:0C:29:BF:B6:0B

Sau khi hoàn tất ta tiến hành khởi chạy máy ảo.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, thiết bị điện tử

Mô tả được tạo tự độngSử dụng phím Enter để lựa chọn cài đặt IPFire.

Hình 3.2.1.3 Giao diện khởi tạo của IPFire

Tiến hành lựa chọn ngôn ngữ sử dụng.

Chấp nhận điều khoản sử dụng của IPFire.

Lựa chọn ngôn ngữ bàn phím.

Lựa chọn múi giờ.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, thiết bị điện tử

Mô tả được tạo tự độngHình 3.2.1.4 Giao diện lựa chọn múi giờ

Đặt tên cho máy chủ và tên Domain.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, máy tính

Mô tả được tạo tự độngĐặt password cho tài khoản root. (ở bước này để đảm bảo tính bảo mật và đề phòng người khác thấy được độ dài của mật khẩu nên sẽ không hiển thị ký tự gì vào ô nhập)

Hình 3.2.1.5 Giao diện thiết lập mật khẩu tài khoản root

Đặt password cho tài khoản admin để đăng nhập trên trang web quản trị.

Tại menu cấu hình mạng, ở bài báo cáo này sẽ thực hiện kiểu cấu hình mạng GREEN, ORANGE và RED.

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, máy tính

Mô tả được tạo tự động

Hình 3.2.1.6 Giao diện cấu hình mạng

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, máy tính

Mô tả được tạo tự độngTại lựa chọn Driver and card assignments, thiết lập chọn địa MAC cho mạng GREEN, RED, ORANGE tương ứng.

Hình 3.2.1.7 Giao diện thiết lập địa chỉ MAC cho mỗi vùng

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình, máy tính

Mô tả được tạo tự độngTại lựa chọn Address settings, thiết lập địa chỉ IP cho GREEN (trong bài này sẽ sử dụng IP cùng dải với IP của VMnet8 là 192.168.1.10)

Hình 3.2.1.8 Thiết lập địa chỉ IP cho GREEN

Tương tự đặt địa chỉ IP cho ORANGE là 192.168.10.1

Đặt địa chỉ cho giao diện RED, ở đây có 3 loại kết nối cho ta lựa chọn.

Static: Đây là chế độ đơn giản nhất, trong đó IPFire được kết nối với mạng Ethernet và được gán một địa chỉ IP tĩnh trong cùng một mạng. Cần phải nắm rõ các thông tin từ nhà cung cấp dịch vụ Internet (ISP): Địa chỉ IP, mặt nạ mạng, địa chỉ cổng kết nối.

DHCP: Đây là thiết lập cho một địa chỉ IP DHCP cho giao diện RED. Thiết bị IPFire được kết nối với mạng và đang cấp phát địa chỉ IP qua giao thức DHCP.

PPP DIALUP: Để kết nối với nhà cung cấp DSL, IPFire cần thông tin đăng nhập để kết nối.

Ở bước này theo bài báo cáo sẽ sử dụng loại kết nối Static.

Đặt địa chỉ IP là 192.168.20.1 và Gateway là 0.0.0.0

Lựa chọn Enable để bật máy chủ DHCP và nhập giá trị bắt đầu và kết thúc của phạm vi IP mong muốn. Phạm vi này phải nằm trong cùng một subnet (phạm vi địa chỉ) như IP của giao diện mạng GREEN.

Trong khuôn khổ bài báo cáo này sẽ không lựa chọn dịch vụ DHCP

### Hướng dẫn cấu hình tường lửa IPFire

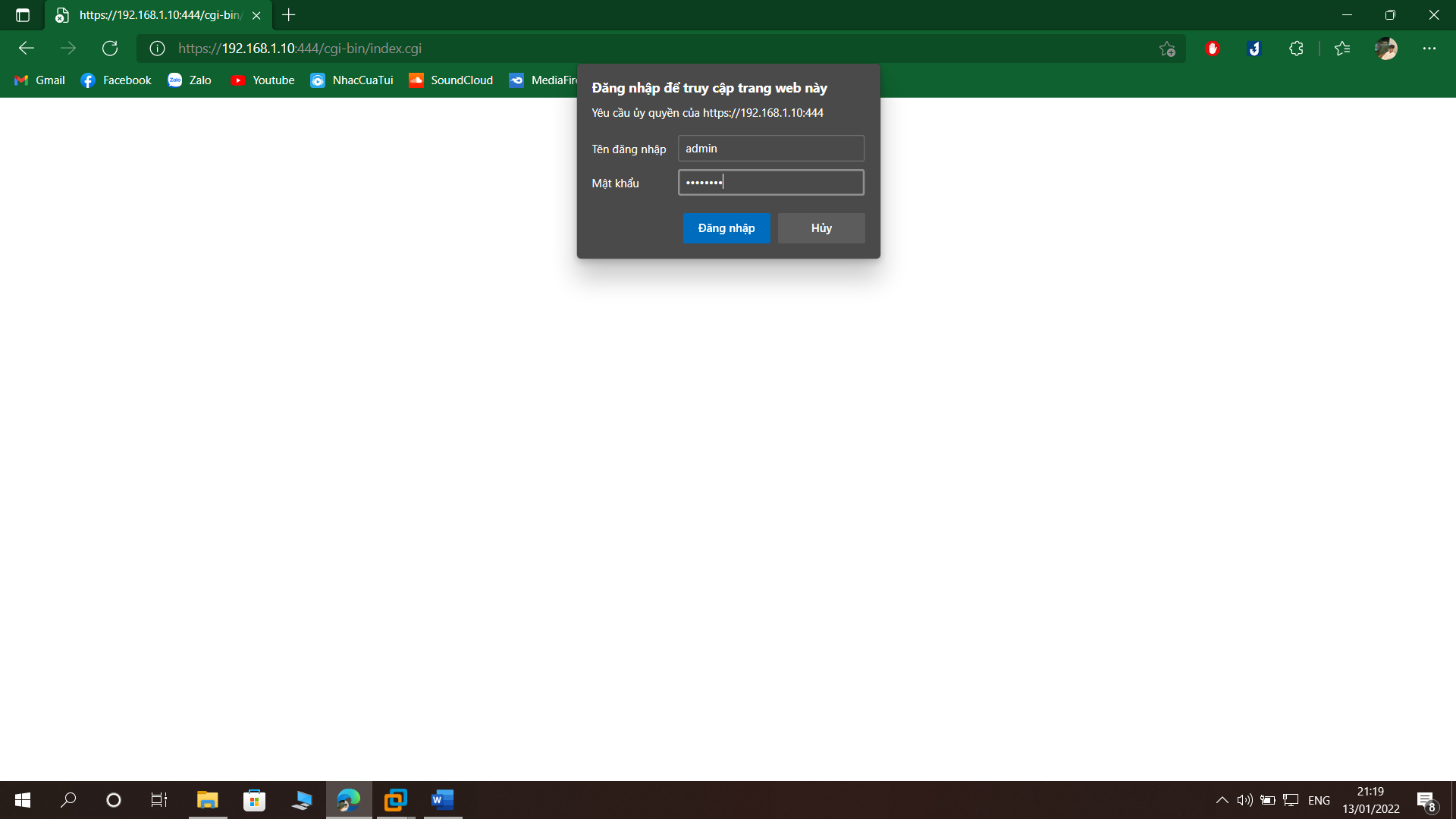
Sau khi cài đặt, ta đăng nhập vào tường lửa IPFire với username: root và password (ở đây sẽ không hiển thị ký tự vì lý do bảo mật) đã thiết lập ở bước trên.

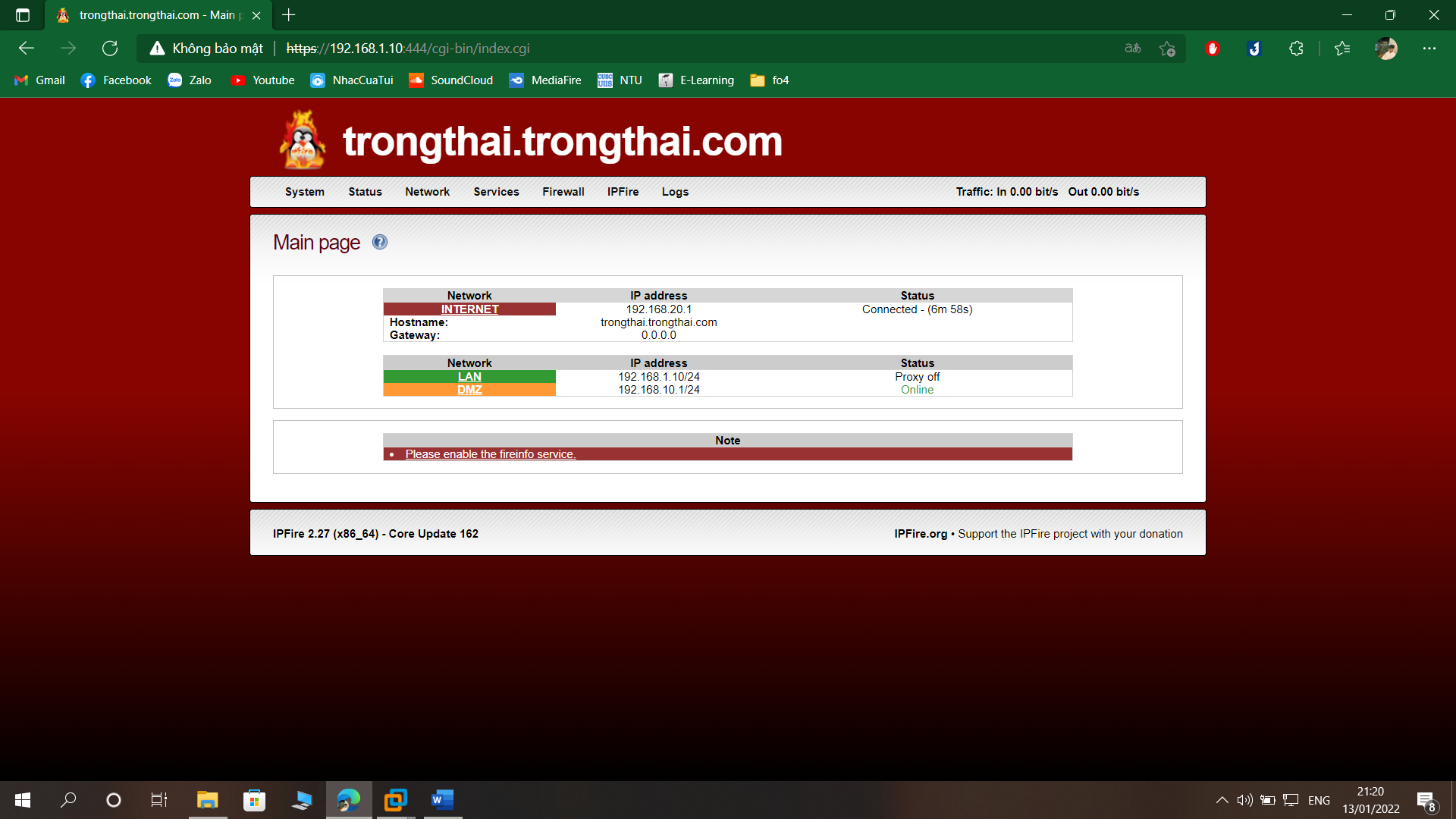
Ảnh có chứa văn bản, ảnh chụp màn hình, thiết bị điện tử, máy tính

Mô tả được tạo tự độngHình 3.2.2.1 Màn hình đăng nhập trên IPFire Linux

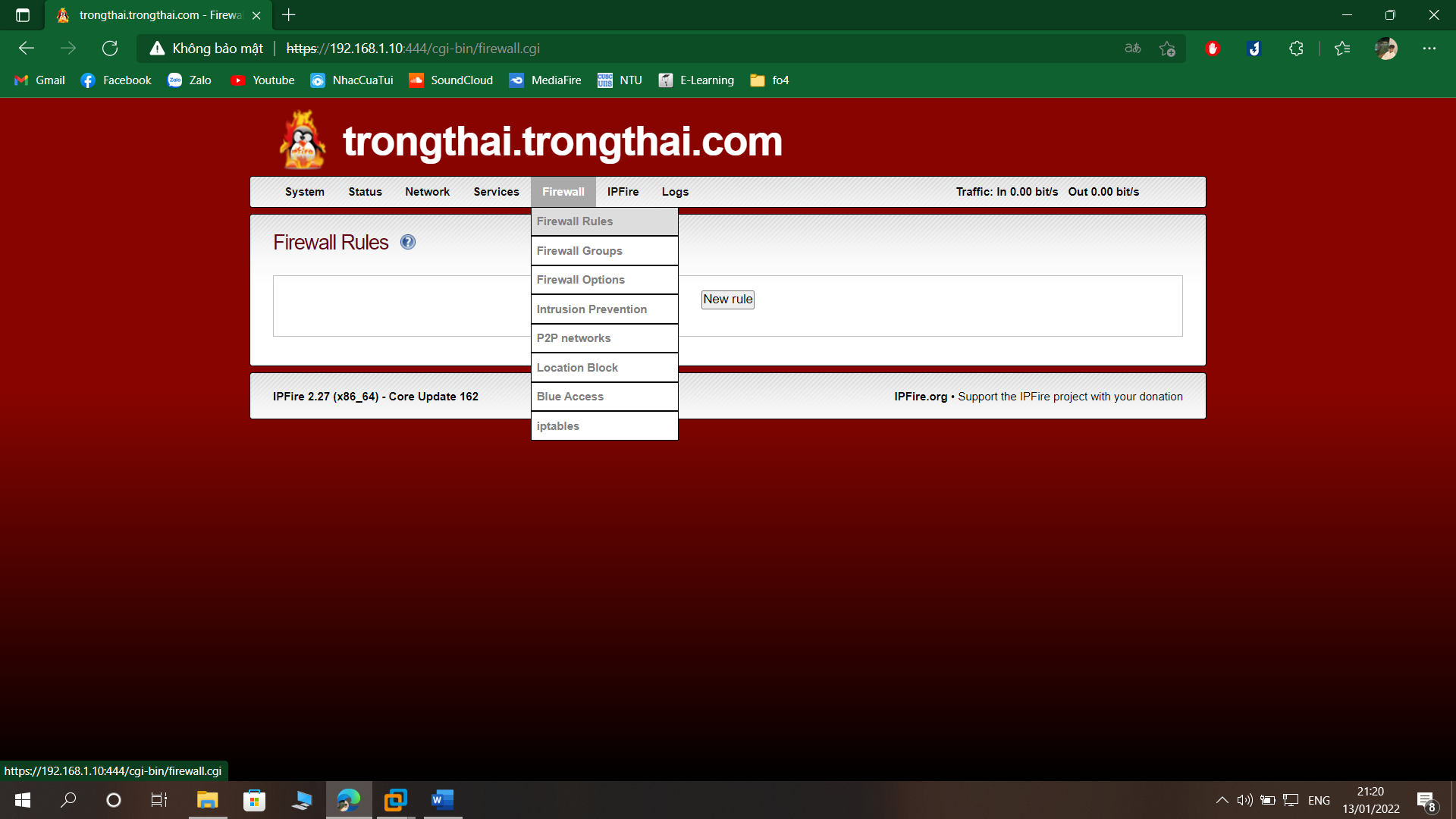
Sử dụng máy thật vào trình duyệt để đăng nhập vào màn hình quản trị với địa chỉ https://192.168.1.10:444 (tại đây trình duyệt sẽ báo là kết nối không an toàn, ta chọn nâng cao và tiếp tục truy cập).

Đăng nhập với tài username: admin và password đã thiết lập trước đó.

Hình 3.2.2.2 Màn hình đăng nhập giao diện quản trị IPFire trên web



Hình 3.2.2.3 Giao diện chính của màn hình quản trị IPFire

Hình 3.2.2.4 Giao diện menu quy tắc tường lửa

Ở đây ta sẽ cấu hình IPFire để thiết lập các quy tắc như:

-NAT là một kỹ thuật được sử dụng để giả mạo (hoặc ẩn) địa chỉ IP của máy chủ chứa gói dữ liệu. Phổ biến nhất là cung cấp dịch vụ từ một địa chỉ IP nhất định.

Ta chọn Firewall -> Firewall Rules và New rule để tạo thêm quy tắc mới.

Source: Chọn địa chỉ IP hoặc máy chủ lưu trữ kết nối được bắt đầu từ đó.

Destination: Trong bước này thể hiện máy chủ đích mà quy tắc này được áp dụng.

Hình 3.2.2.5

-Chặn

## HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA PFsense

### Hướng dẫn cài đặt tường lửa PFsense

Tương tự IPFire, ta download PFsense tại trang chủ [www.pfsense.org](http://www.pfsense.org)

Tạo một máy ảo mới với 2 card mạng.

VMnet10: Thiết lập IP 192.168.10.0 cho mạng LAN

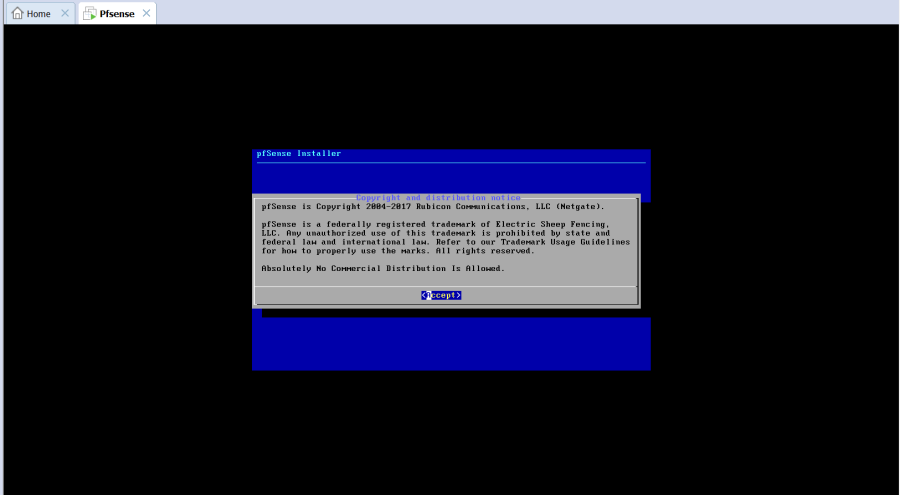
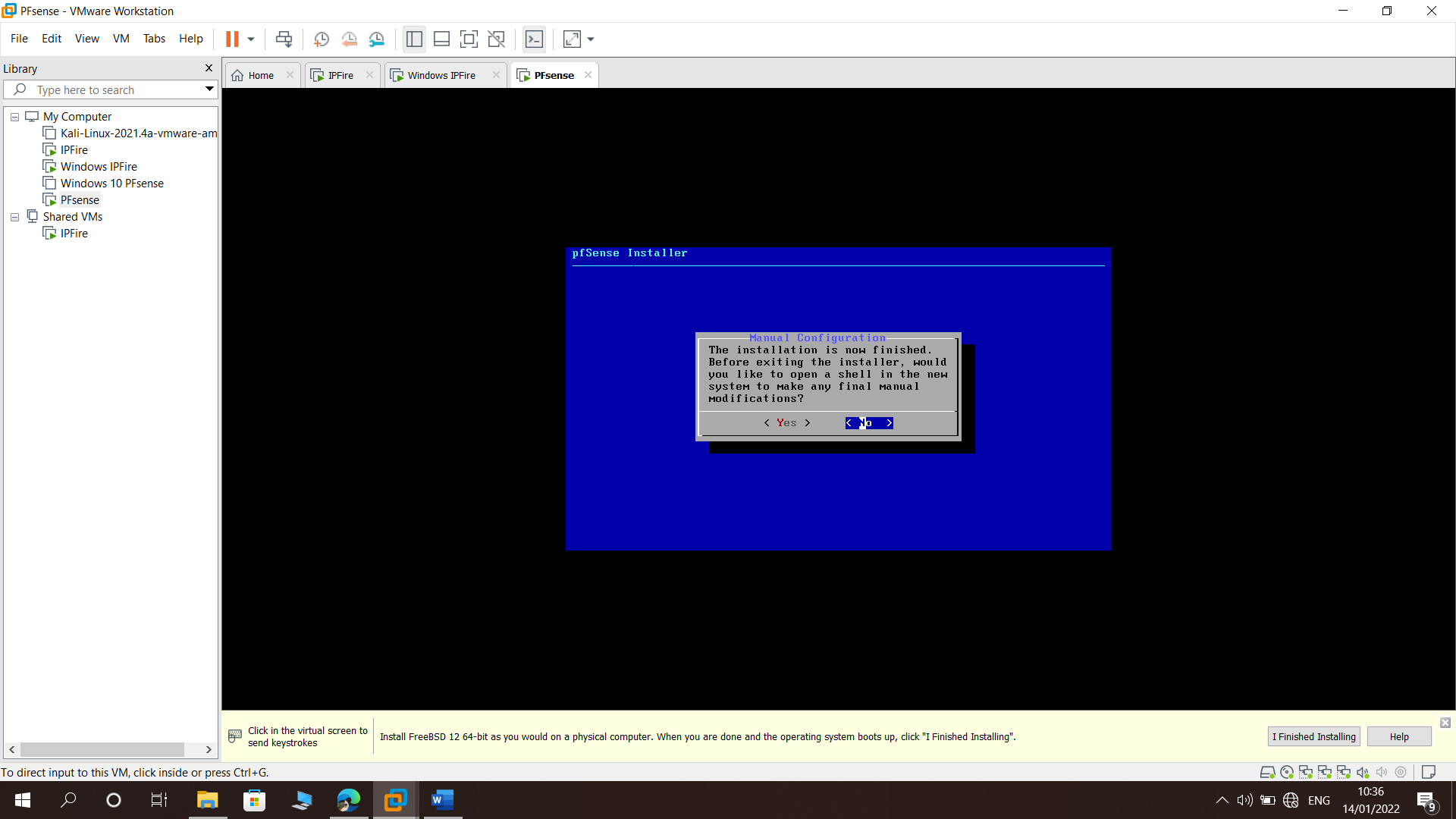
VMnet9: Là vùng Internet bên ngoài - WAN

Ảnh có chứa văn bản, ảnh chụp màn hình, máy tính

Mô tả được tạo tự động

Khởi chạy PFsense vừa tạo, tại đây PFsense sẽ tự chọn mode khởi động .

Hình 3.3.1.1 Giao diện điều khoản PFsense



Nhấn Accecpt để chấp nhận.

Nhấn OK để cài đặt PFsense.

Ảnh có chứa văn bản, màn hình, ảnh chụp màn hình, máy tính

Mô tả được tạo tự độngHình 3.3.1.2 Giao diện cài đặt

Tại bước này chọn No và Reboot lại hệ thống.

Sau khi Reboot hệ thống sẽ vào giao diện cài đặt ban đầu.

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết bị điện tử, màn hình

Mô tả được tạo tự độngHình 3.3.1.3 Giao diện cài đặt

Tại đây ta nhập “2” để lựa chọn thiết lập IP cho Interface LAN

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết bị điện tử, máy tính

Mô tả được tạo tự độngHình 3.3.1.4 Giao diện thiết lập interface

Tiếp tục nhập “2” để lựa chọn thiết lập IP cho LAN, sau đó nhập IP cùng dải với IP LAN của card mạng Vmnet10 là 192.168.10.1 sau đó nhấn Enter.

Lựa chọn Subnetmask là 24.

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết bị điện tử, màn hình

Mô tả được tạo tự độngBấm Enter để bỏ qua Ipv6.

Hình 3.3.1.5 Giao diện thiết lập DHCP

Nhập “n” để không thiết lập DHCP cho LAN, nhập “y” để đồng ý lựa chọn revert to DHCP.

Sau khi hoàn tất ta truy cập PFsense ở máy chính tại địa chỉ http://192.168.10.1/

### Hướng dẫn cấu hình tường lửa PFsense

Sử dụng máy thật vào trình duyệt để đăng nhập vào màn hình quản trị với địa chỉ <http://192.168.10.1/>

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự độngĐăng nhập với tài username: admin và password: pfsense.

Hình 3.3.2.1 Màn hình đăng nhập PFsense trên web

Ảnh có chứa văn bản

Mô tả được tạo tự độngSau khi đăng nhập ta tiến hành đổi mật khẩu và cấu hình cơ bản.

Hình 3.3.2.2 Màn hình thiết lập ban đầu

Đặt hostname và Domain, đặt địa chỉ DNS server.

Thiết lập WAN interface, lựa chọn static. Đặt IP WAN là 192.168.1.20 (cùng dải với máy thật vì dùng chung 1 card mạng), subnet mask là 24 và gateway là 192.168.1.1

# THỰC HIỆN BÀI KIỂM TRA VỀ ĐỘ BẢO MẬT

## HƯỚNG DẪN CÀI ĐẶT Kali Linux

…

## THỰC HIỆN KIỂM THỬ LỖ HỔNG BẢO MẬT

### Kiểm thử lỗ hổng bảo mật trên IPFire

### Kiểm thử lỗ hổng bảo mật trên PFsense

# KẾT QUẢ

## KẾT QUẢ ĐẠT ĐƯỢC

…

## ƯU ĐIỂM CỦA TƯỜNG LỬA IPFire

…

## HẠN CHẾ CỦA TƯỜNG LỬA IPFire

…

## KẾT LUẬN

…

# TÀI LIỆU THAM KHẢO

# PHỤ LỤC

## Phụ lục 1: