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](#_Toc92029019)

[TÓM TẮT ĐỒ ÁN ii](#_Toc92029020)

[MỤC LỤC iii](#_Toc92029021)

[DANH MỤC HÌNH VẼ iv](#_Toc92029022)

[DANH MỤC BẢNG iv](#_Toc92029023)

[DANH MỤC CÁC TỪ VIẾT TẮT v](#_Toc92029024)

[MỞ ĐẦU 1](#_Toc92029025)

[Chương 1. TỔNG QUAN VỀ VẤN ĐỀ NGHIÊN CỨU 3](#_Toc92029026)

[1.1 CƠ SỞ LÝ THUYẾT 3](#_Toc92029027)

[1.1.1 Tổng quan về tường lửa 3](#_Toc92029028)

[1.1.2 Tổng quan về công nghệ ảo hóa VMware 6](#_Toc92029029)

[1.1.3 Tổng quan về Kali Linux 6](#_Toc92029030)

[1.2 CÁC PHƯƠNG PHÁP KIỂM THỬ LỖ HỔNG BẢO MẬT 6](#_Toc92029031)

[1.2.1 Phương pháp 1 6](#_Toc92029032)

[1.2.2 Phương pháp 2 7](#_Toc92029033)

[1.3 THỰC TIỄN VẤN ĐỀ LIÊN QUAN ĐẾN ĐỀ TÀI 8](#_Toc92029034)

[1.4 TỔNG QUAN TÌNH HÌNH NGHIÊN CỨU 8](#_Toc92029035)

[1.4.1 Tình hình nghiên cứu trên thế giới 8](#_Toc92029036)

[1.4.2 Tình hình nghiên cứu trong nước 8](#_Toc92029037)

[Chương 2. TỔNG QUAN VỀ TƯỜNG LỬA IPFire 9](#_Toc92029038)

[2.1 TƯỜNG LỬA IPFire 9](#_Toc92029039)

[2.2 NHỮNG CHỨC NĂNG CHÍNH CỦA TƯỜNG LỬA IPFire 9](#_Toc92029040)

[Chương 3. CẤU HÌNH VÀ CÀI ĐẶT TƯỜNG LỬA IPFire, PFsense 10](#_Toc92029041)

[3.1 HƯỚNG DẪN CÀI ĐẶT PHẦN MỀM HỖ TRỢ ẢO HÓA VMware 10](#_Toc92029042)

[3.2 HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA IPFire 10](#_Toc92029043)

[3.2.1 Hướng dẫn cài đặt tường lửa IPFire 10](#_Toc92029044)

[3.2.2 Hướng dẫn cấu hình tường lửa IPFire 10](#_Toc92029045)

[3.3 HƯỚNG DẪN CÀI ĐẶT VÀ CẤU HÌNH TƯỜNG LỬA PFsense 10](#_Toc92029046)

[3.3.1 Hướng dẫn cài đặt tường lửa PFsense 10](#_Toc92029047)

[3.3.2 Hướng dẫn cấu hình tường lửa PFsense 10](#_Toc92029048)

[Chương 4. THỰC HIỆN BÀI KIỂM TRA VỀ ĐỘ BẢO MẬT 10](#_Toc92029049)

[4.1 HƯỚNG DẪN CÀI ĐẶT Kali Linux 10](#_Toc92029050)

[4.2 THỰC HIỆN KIỂM THỬ LỖ HỔNG BẢO MẬT 10](#_Toc92029051)

[4.2.1 Kiểm thử lỗ hổng bảo mật trên IPFire 10](#_Toc92029052)

[4.2.2 Kiểm thử lỗ hổng bảo mật trên PFsense 10](#_Toc92029053)

[Chương 5. KẾT QUẢ 11](#_Toc92029054)

[5.1 KẾT QUẢ ĐẠT ĐƯỢC 11](#_Toc92029055)

[5.2 ƯU ĐIỂM CỦA TƯỜNG LỬA IPFire 11](#_Toc92029056)

[5.3 HẠN CHẾ CỦA TƯỜNG LỬA IPFire 11](#_Toc92029057)

[5.4 KẾT LUẬN 11](#_Toc92029058)

[TÀI LIỆU THAM KHẢO 11](#_Toc92029059)

[PHỤ LỤC 11](#_Toc92029060)

[1. Phụ lục 1: 11](#_Toc92029061)

# DANH MỤC HÌNH VẼ

# DANH MỤC BẢNG

# 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

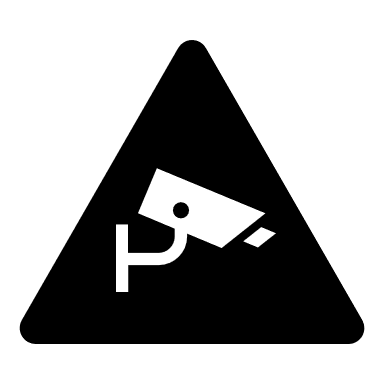
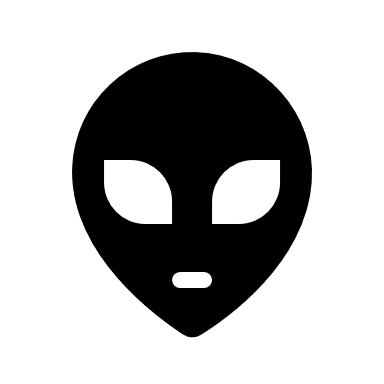
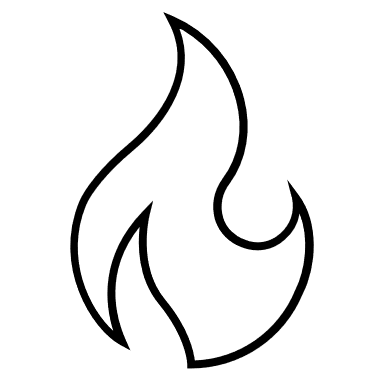
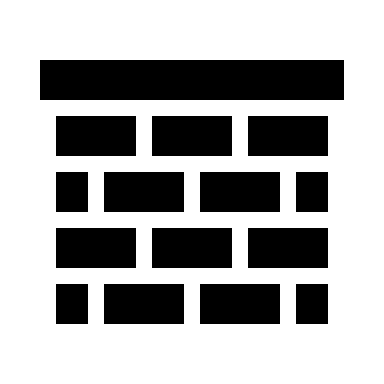
## CƠ SỞ LÝ THUYẾT

### 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.

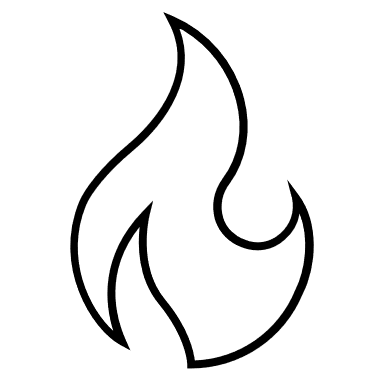
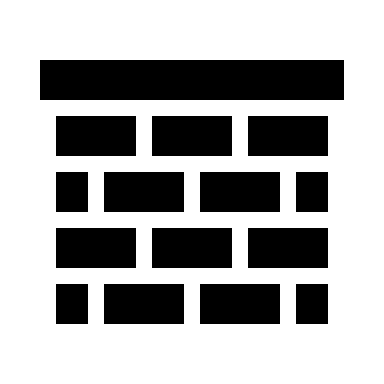


Mạng nội bộ (LAN)

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

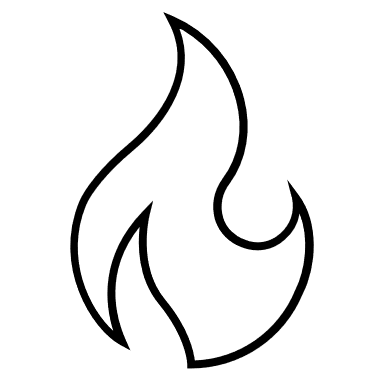
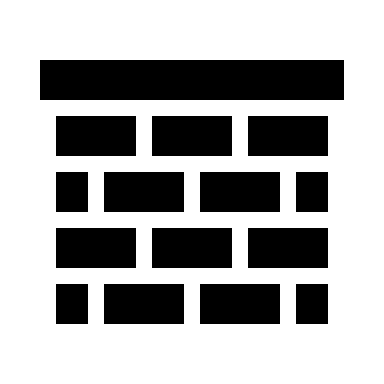
Tường lửa hoạt động theo cách kiểm tra thông tin vào và ra Internet. Nó nhận dạng và từ chối truy cập các thông tin tới tự những địa chỉ nguy hiểm hoặc có vẻ nghi ngờ. Tường lửa là một giải pháp dựa trên phần cứng hoặc phần mềm dùng để kiểm tra các thông tin. Tường lửa là một giải pháp cần phải có cho 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 Firewall cho mạng nội bộ có phân đoạn mạng



Ban kiểm toán

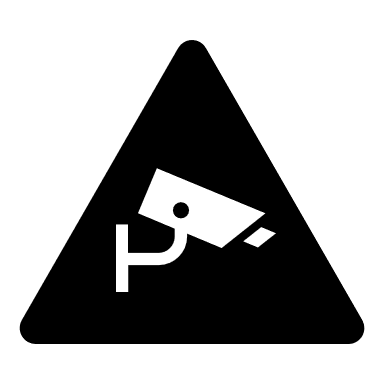
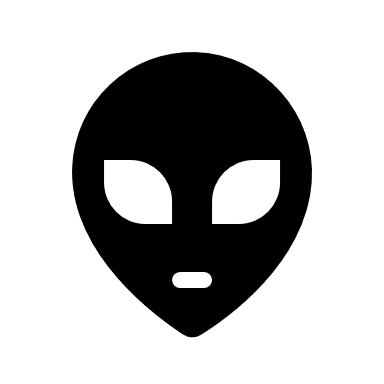
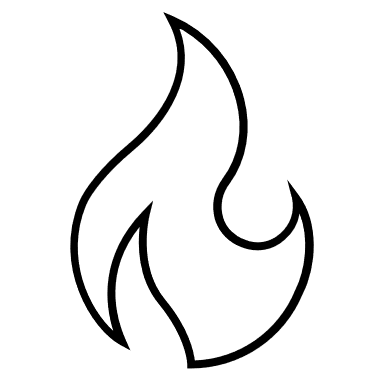
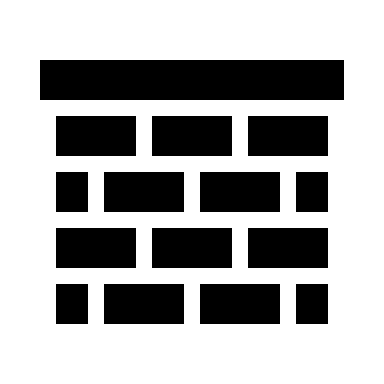


Ban sản xuất

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

…

#### Mục đích của VMware Workstation

…

#### Chức năng của VMware Workstation

…

### 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

### Phương pháp 1

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

### Phương pháp 2

…

## 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

…

### Hướng dẫn cấu hình tường lửa IPFire

…

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

### Hướng dẫn cài đặt tường lửa PFsense

…

### Hướng dẫn cấu hình tường lửa PFsense

…

# 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: