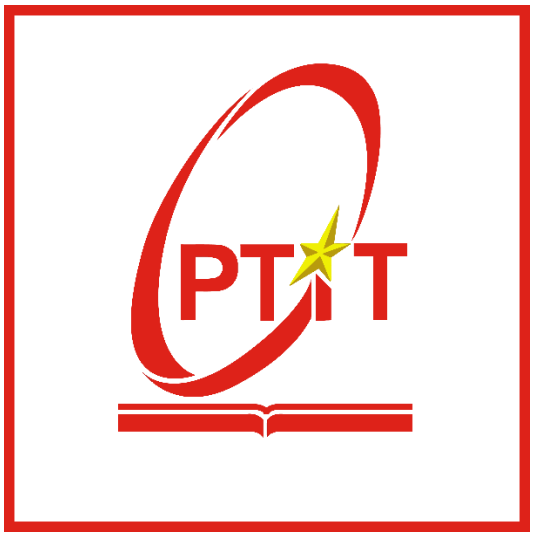
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN



Môn học: **THỰC TẬP CƠ SỞ**

BÁO CÁO BÀI THỰC HÀNH SỐ 5

CÀI ĐẶT, CẤU HÌNH MẠNG DOANH NGHIỆP VỚI PFSENSE FIREWALL

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 3/2024 ~

Mục Lục

BÀI 5: Cài đặt, cấu hình mạng doanh nghiệp với Pfsense firewall

1 Mục đích

Các công ty thường bảo vệ hệ thống mạng bằng cách sử dụng tường lửa phần cứng hoặc phần mềm để kiểm soát lưu lượng mạng truy cập. Một số loại lưu lượng nhất định có thể bị chặn hoặc cho phép đi qua tường lửa. Việc hiểu cách thức hoạt động của tường lửa và mối quan hệ của nó với các mạng bên trong và bên ngoài sẽ rất quan trọng để có hiểu biết về bảo mật mạng.

Bài thực hành này giúp sinh viên có thể tự cài đặt, xây dựng một mạng doanh nghiệp với tường lửa để kiểm soát truy cập. Mạng mô phỏng môi trường mạng doanh nghiệp này có thể sử dụng trong các bài lab về ATTT sau này.

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

2.1.1 Cấu hình mạng trong phần mềm mô phỏng Vmware/Virtualbox

a) VMware

Vmware Workstation cung cấp khả năng tạo mạng riêng, mạng cô lập, cung cấp máy chủ DHCP sử dụng để phân phối địa chỉ IP cho các máy ảo chạy trên đó. Ngoài ra có thể đặt giới hạn đến cũng như lưu lượng đi cho các máy ảo.

Có 3 mạng mặc định được tạo khi cài đặt Vmware Workstation: VMnet0, VMnet1, Vmnet8. Chúng thuộc các loại khác nhau: Bridged, Host-only, NAT.

- Mạng Bridged: máy ảo sẽ hoạt động như một máy ảo độc lập được kết nối với bộ chuyển mạch hoặc bộ định tuyến vật lý. Máy ảo này sẽ trực tiếp lấy địa chỉ IP từ máy chủ DHCP. Khi sử dụng mạng bridged, máy ảo sẽ tham gia đầy đủ vào mạng, có quyền truy cập vào các máy khác trong mạng và có thể được liên lạc với các máy khác trong mạng như một máy tính vật lý trong mạng. Khi sử dụng card mạng này IP của máy ảo sẽ cùng với dải IP của máy thật.

- Mạng NAT: đây là mạng mặc định được sử dụng và gán khi tạo 1 máy ảo mới. Trong mạng NAT, máy ảo sẽ không có địa chỉ IP riêng trên mạng bên ngoài. Thay vào đó, một mạng riêng biệt được thiết lập trên máy tính chủ. Máy ảo sẽ nhận một địa chỉ trên mạng đó từ máy chủ DHCP ảo Vmware. Thiết bị Vmware NAT truyền dữ liệu mạng giữa một hoặc nhiều máy ảo và mạng bên ngoài, nó xác định các gói dữ liệu đến dành cho mỗi máy ảo và gửi chúng đến đúng đích.

- Mạng Host-only: dùng để tạo một mạng hoàn toàn biệt lập để máy ảo không thể thấy các mạng khác hoặc internet. Mạng này cung cấp kết nối mạng giữa máy ảo và máy tính chủ, sử dụng bộ điều hợp Ethernet ảo hiển thị cho hệ điều hành máy chủ.

Vmware Workstation hỗ trợ tối da từ 0 đến 19 bộ điều hợp Vmnet.

b) VirtualBox

VirtualBox cung cấp một danh sách dài các chế độ mạng. Mỗi bộ điều hợp mạng ảo có thể được cấu hình riêng biệt để hoạt động ở một chế độ mạng khác nhau. Các chế độ mạng của VirtualBox:

- Not Attached: chế độ không kết nối mạng cho máy ảo.

- NAT Network: Chế độ này tương tự như chế độ NAT, sử dụng để cấu hình bộ định tuyến. Sử dụng NAT Network cho nhiều máy ảo, chúng có thể giao tiếp với nhau qua mạng. Các máy ảo có thể truy cập các máy chủ khác trong mạng vật lý và có thể truy cập các mạng bên ngoài bao gồm cả internet. Bất kỳ máy nào từ mạng bên ngoài cũng như từ mạng vật lý mà máy chủ được kết nối không thể truy cập vào các máy ảo được cấu hình để sử dụng chế độ này. Khi sử dụng chế độ này, không thể truy cập máy khách từ máy chủ khi sử dụng. Bộ định tuyến VirtualBox NAT tích hợp sẵn sử dụng bộ điều khiển giao diện mạng vật lý của máy chủ VirtualBox làm giao diện mạng bên ngoài.

- Internal Network: (mạng nội bộ) VirtualBox được kết nối với một mạng ảo biệt lập. Các máy ảo được kết nối với mạng này có thể giao tiếp với nhau, nhưng chúng không thể giao tiếp với máy chủ VirtualBox hoặc với bất kỳ máy chủ nào khác trong mạng vật lý hoặc trong mạng bên ngoài. Máy ảo được kết nối với mạng nội bộ không thể được truy cập từ máy chủ lưu trữ hoặc bất kỳ thiết bị nào khác.

- Generic Driver: Chế độ mạng này cho phép chia sẻ giao diện mạng chung. Người dùng có thể chọn trình điều khiển thích hợp để được phân phối trong một gói mở rộng hoặc được bao gồm trong VirtualBox. Chế độ này gồm 2 chế độ phụ:

+ UDP Tunnel: Các máy ảo chạy trên các máy chủ khác nhau có thể giao tiếp minh bạch bằng cách sử dụng cơ sở hạ tầng mạng hiện có.

+ VDE Networking: Máy ảo có thể kết nối với công tắc phân tán ảo trên máy chủ Linux hoặc FreeBSD.

2.1.2 Phần mềm Pfsense

Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạnh và miễn phí, ứng dụng này cho phép mở rộng mạng của cơ quan, tổ chức , … mà không bị thỏa hiệp về sự bảo mật. Ứng dụng này có một cộng đồng phát triển rất tích cực và nhiều tính năng đang được bổ sung trong mỗi phát hành nhằm cải thiện hơn nữa tính bảo mật, sự ổn định và khả năng linh hoạt của nó. PfSense bao gồm nhiều tính năng giống nhưcác thiết bị tường lửa hoặc router thương mại, chẳng hạn như GUI trên nền Web tạo sự quản lý một cách dễ dàng.

Pfsense được dựa trên FreeBSD và giao thức Common Address Redundancy Protocol (CARP) của FreeBSD, cung cấp khả năng dự phòng bằng cách cho phép các quản trị viên nhóm hai hoặc nhiều tường lửa vào một nhóm tự động chuyển đổi dự phòng. Vì nó hỗ trợ nhiều kết nối mạng diện rộng (WAN) nên có thể thực hiện việc cân bằng tải. Đặc thù PfSense là tường lửa ngăn các nguy hại giữa mạng WAN và mạng LAN nên máy cài đặt PfSense yêu cầu tối thiểu 2 card mạng.

Các tính năng trong pfsense:

- Aliases: 1Aliases sẽ gom nhóm các IP, Port hoặc URL vào với nhau, 1 alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL.

- NAT: Pfsense có hỗ trợ nat static dưới dạng nat 1:1. IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng.

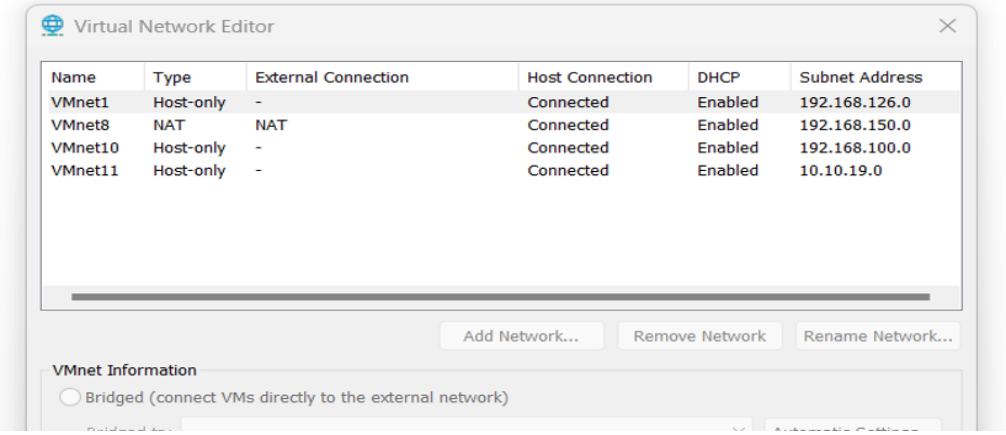
- Firewall Rules: Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào.

- Traffic shaper: giúp quản trị mạng có thể tinh chỉnh, tối ưu hóa đường truyền trong pfsense.

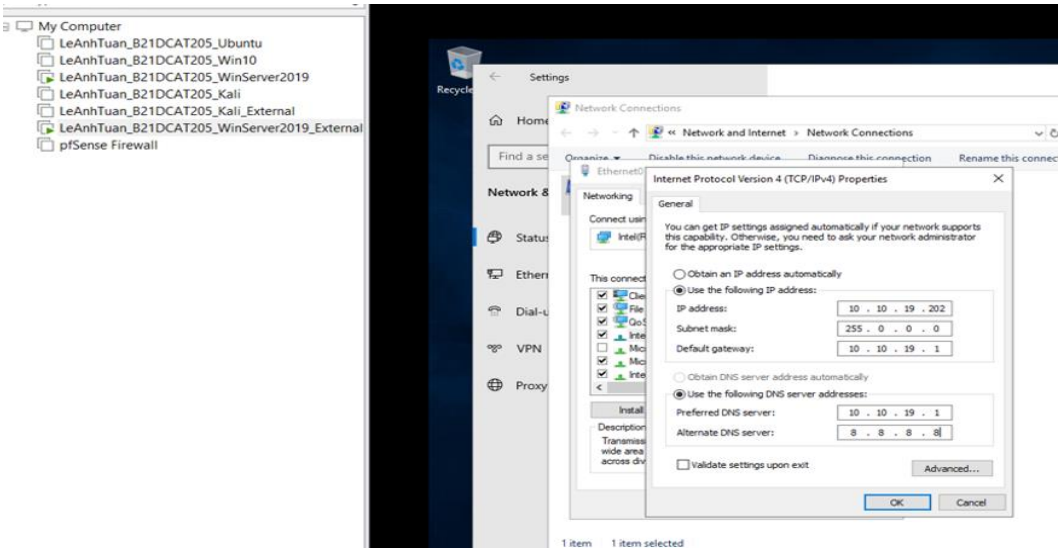
2.2 Cài đặt

2.2.1 Cấu hình Topo mạng

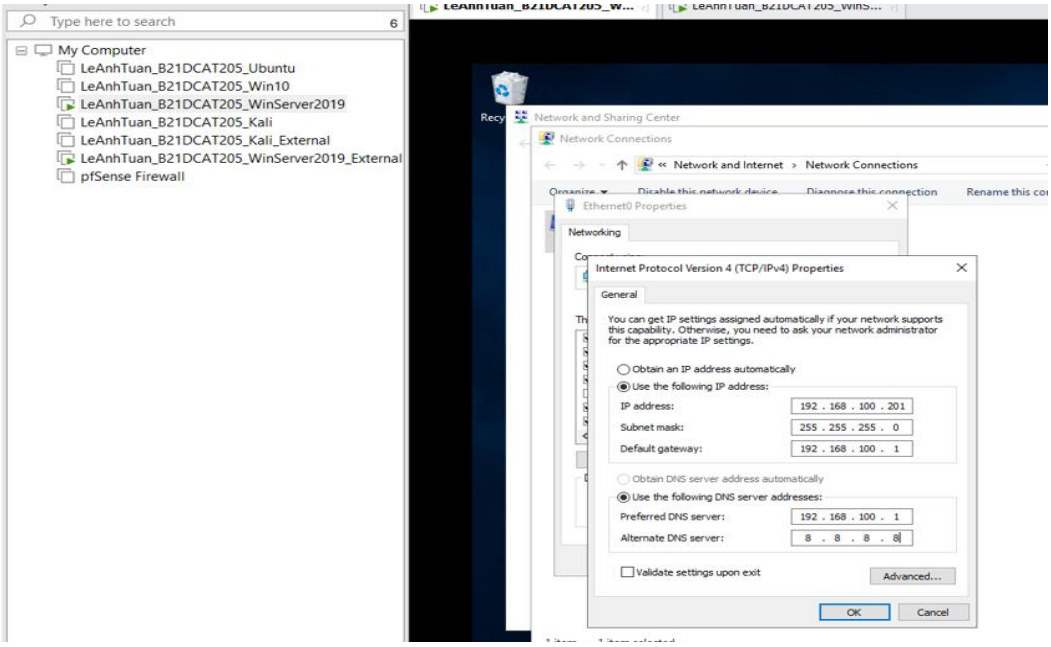
Tạo 2 Subnet trên vmware vmnet11 có địa chỉ 10.10.19.0/24 cho mạng Internal và vmnet10 có địa chỉ 192.168.100.0/24 cho mạng External:



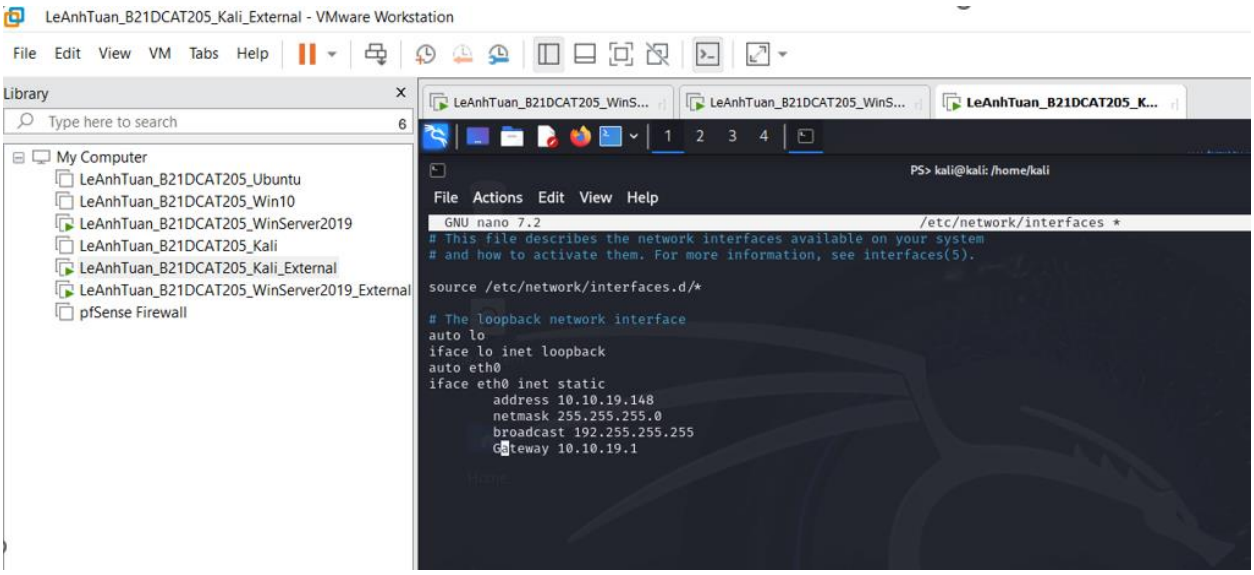
Hình 1: Virtual Network Editor



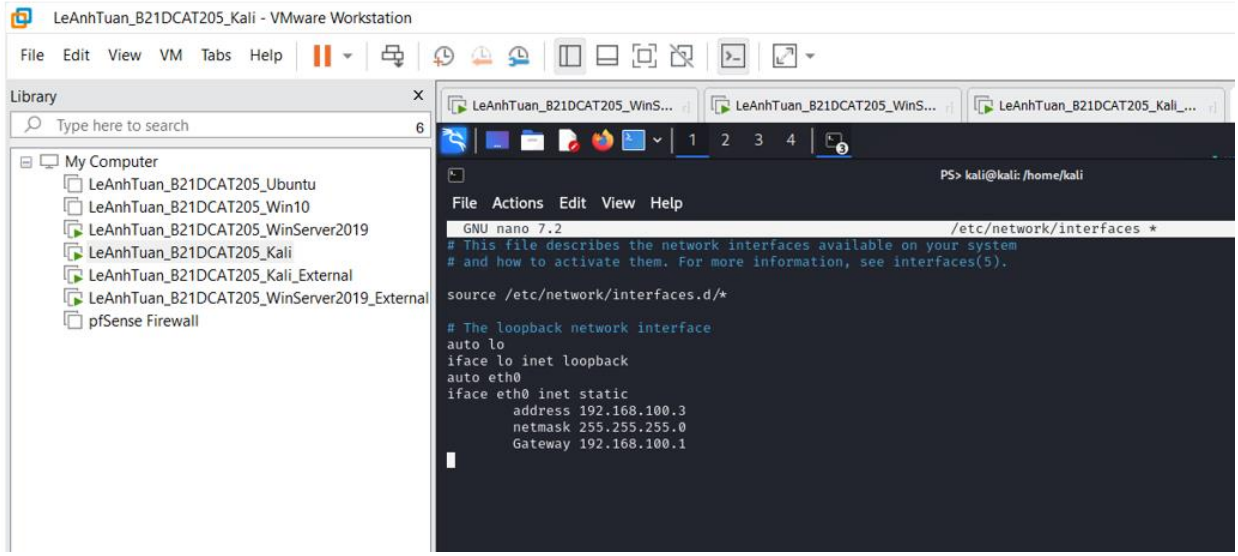
Hình 2: Cấu hình máy Windows Server 2019 mạng External



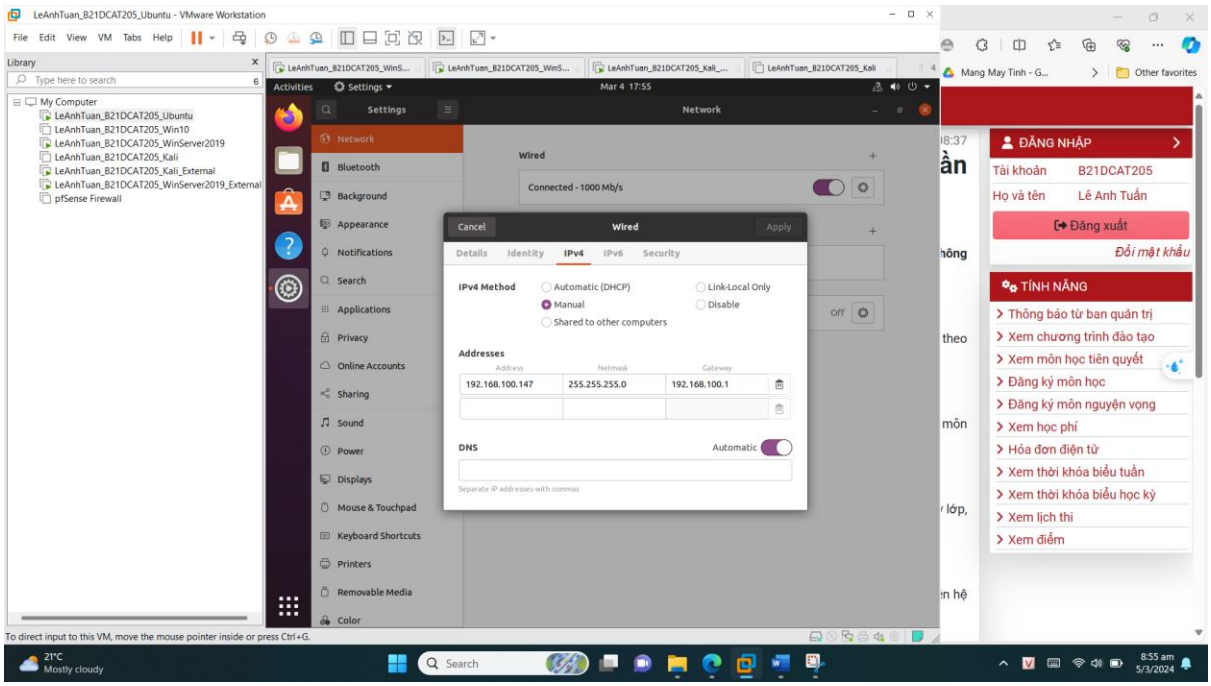
Hình 3: Cấu hình máy Windows Server 2019 mạng Internal



Hình 4: Cấu hình địa chỉ IP (10.10.19.148) cho Kali Linux External

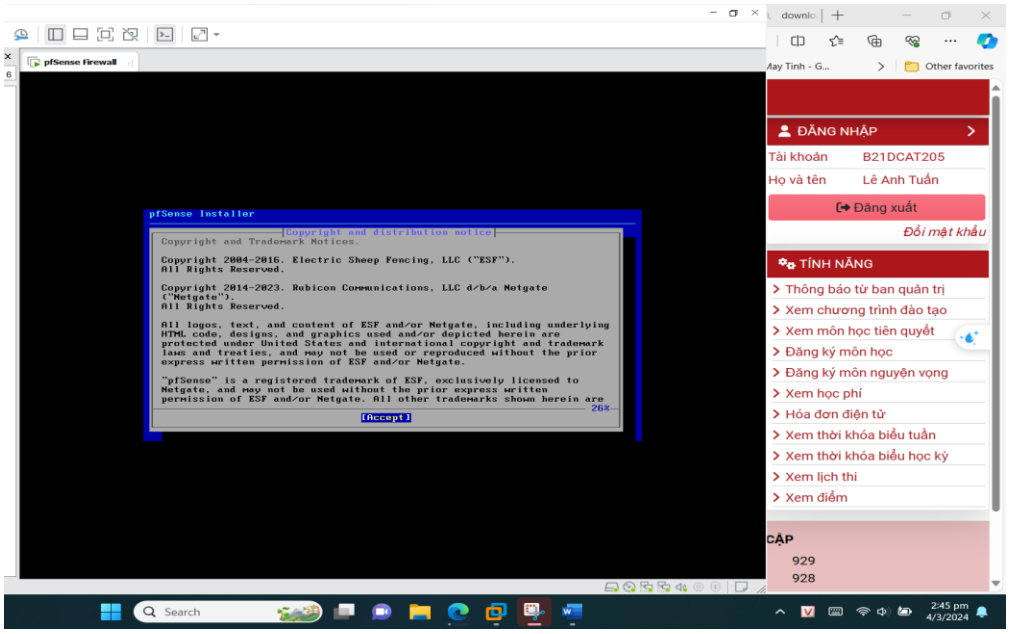


Hình 5: Cấu hình địa chỉ IP (192.168.100.3) cho Kali Linux Internal

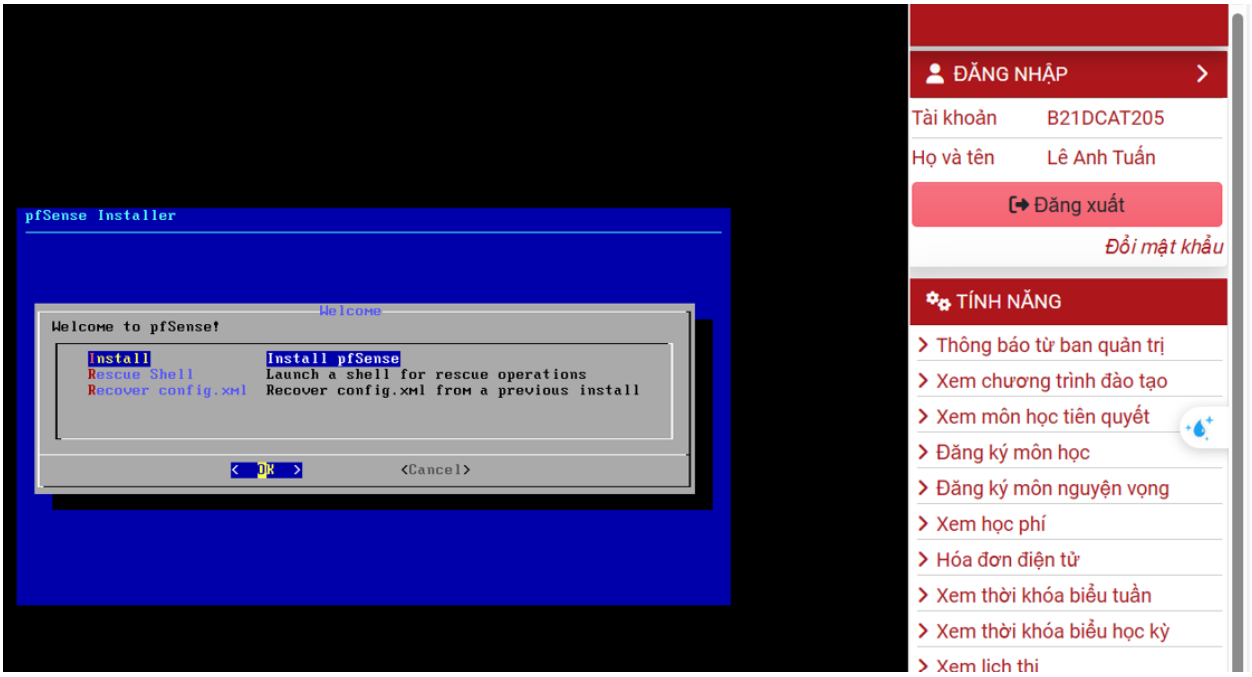


Hình 6: Cấu hình địa chỉ IP (192.168.100.147) cho Ubuntu Linux Internal

Cài đặt máy ảo tường lửa pfSense

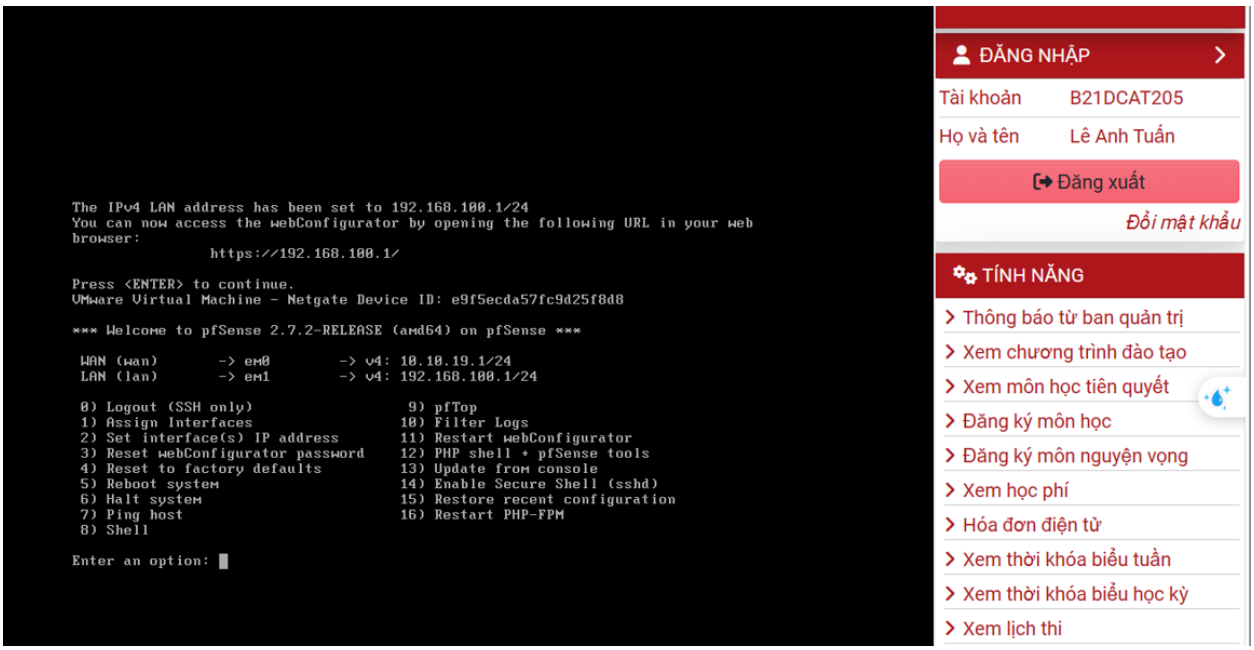


Hình 7: Chọn Accept



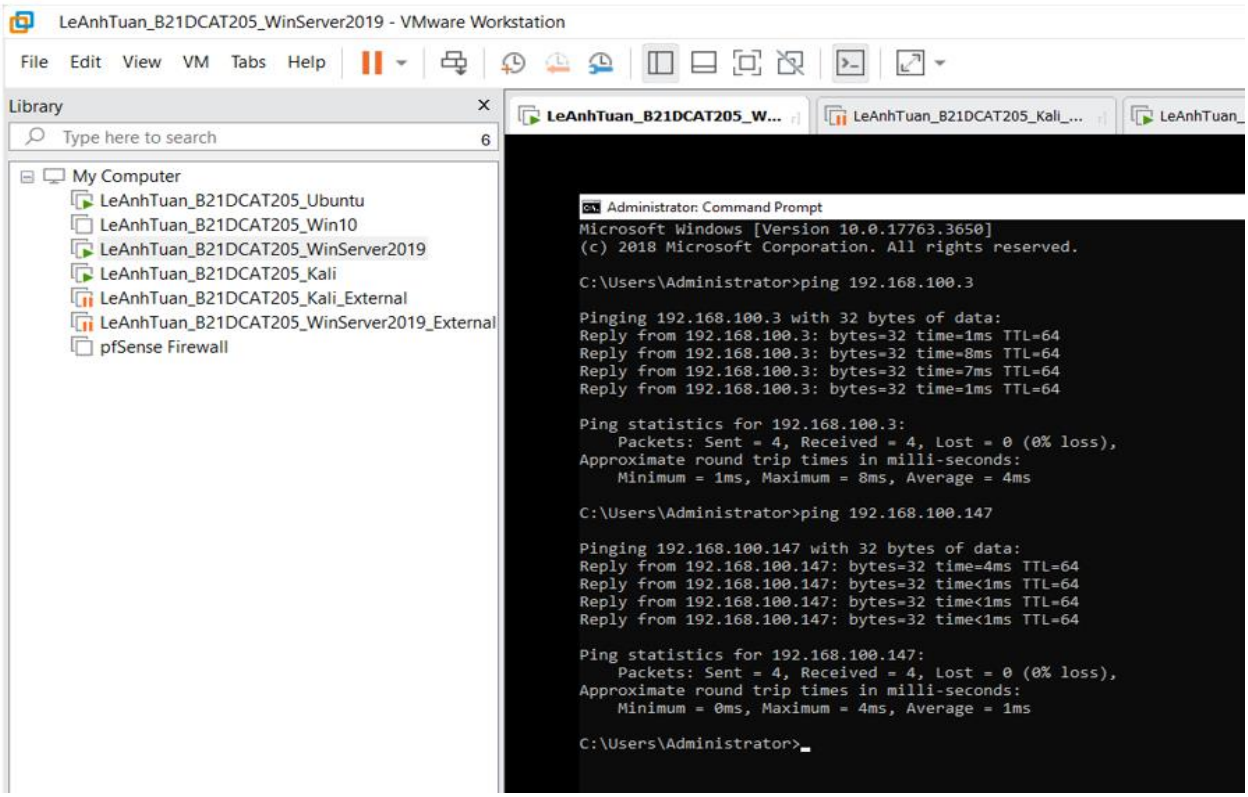
Hình 8: Nhấn Install để cài đặt pfSense

Bấm lựa chọn 2 để cấu hình cho mạng Wan và Lan, ta được kết quả như sau:

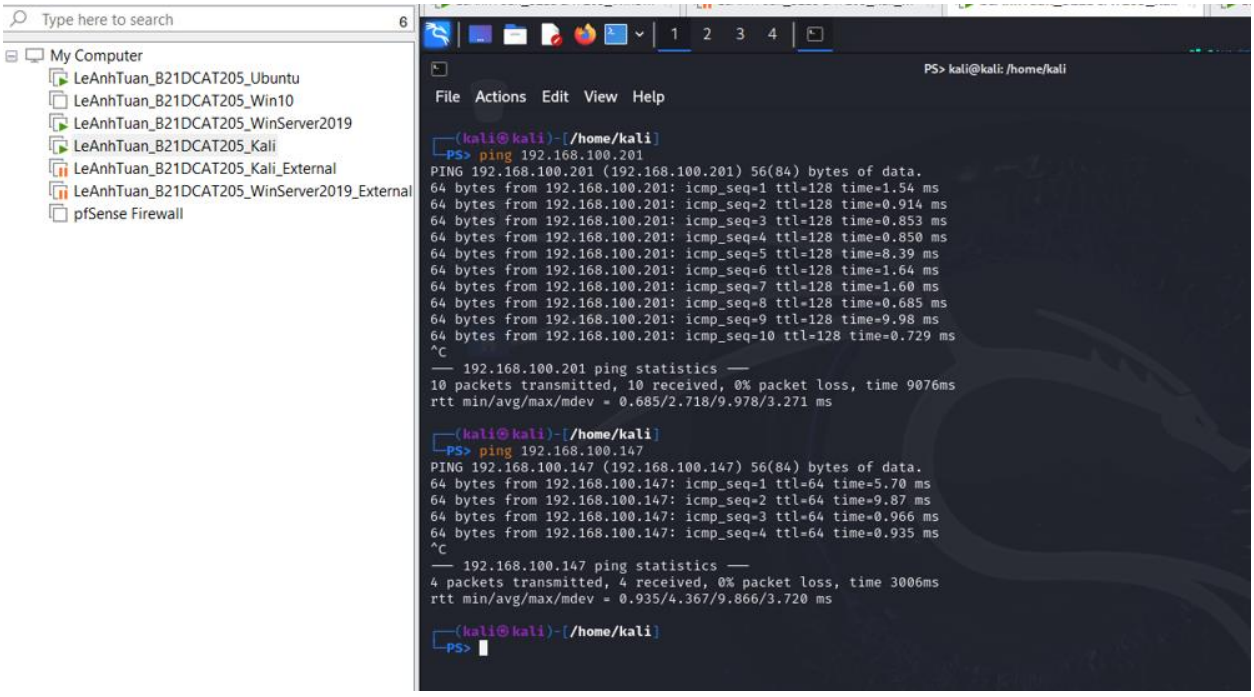


Hình 9: Kết quả sau khi cấu hình

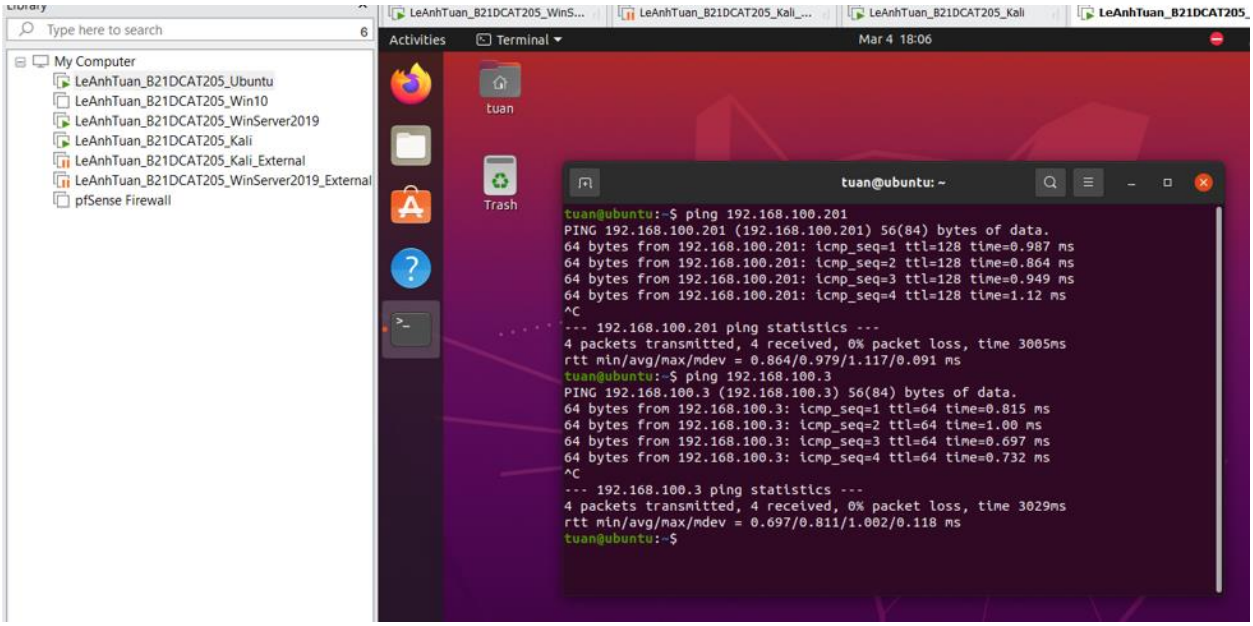
Thử ping các máy cho nhau trong mạng internal



Hình 10: Ping máy Windows Server 2019 internal với Kali internal và Ubuntu internal

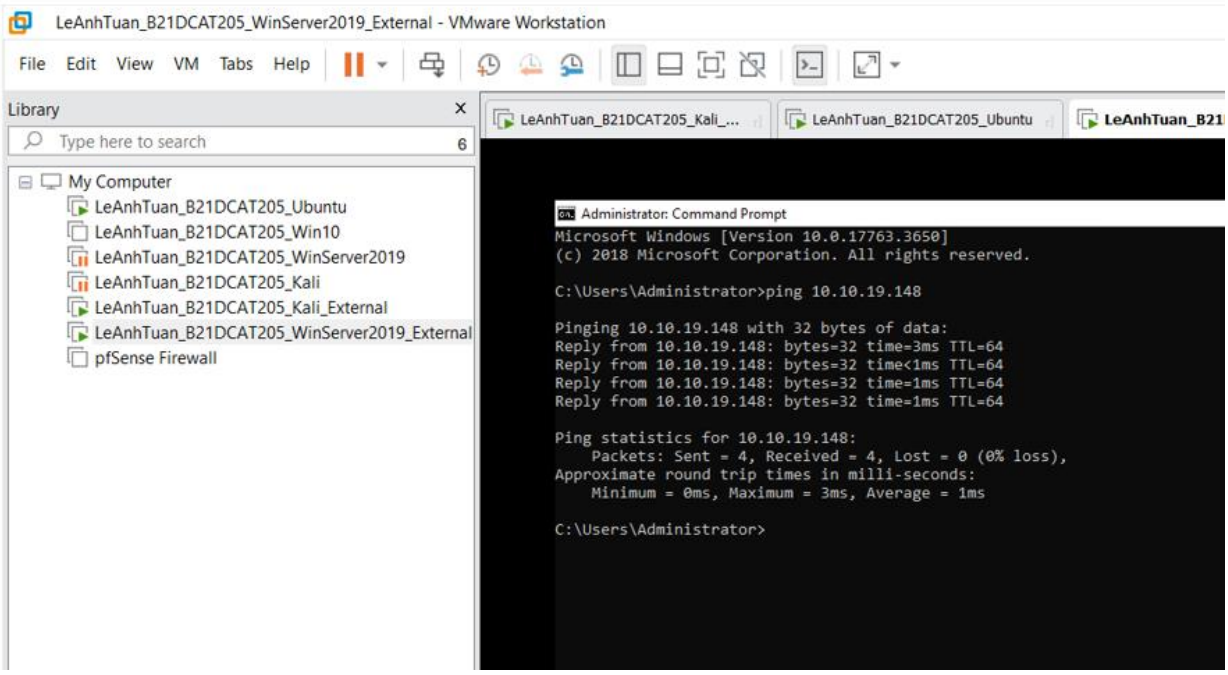


Hình 11: Ping máy Kali internal với Windows Server 2019 internal và Ubuntu internal

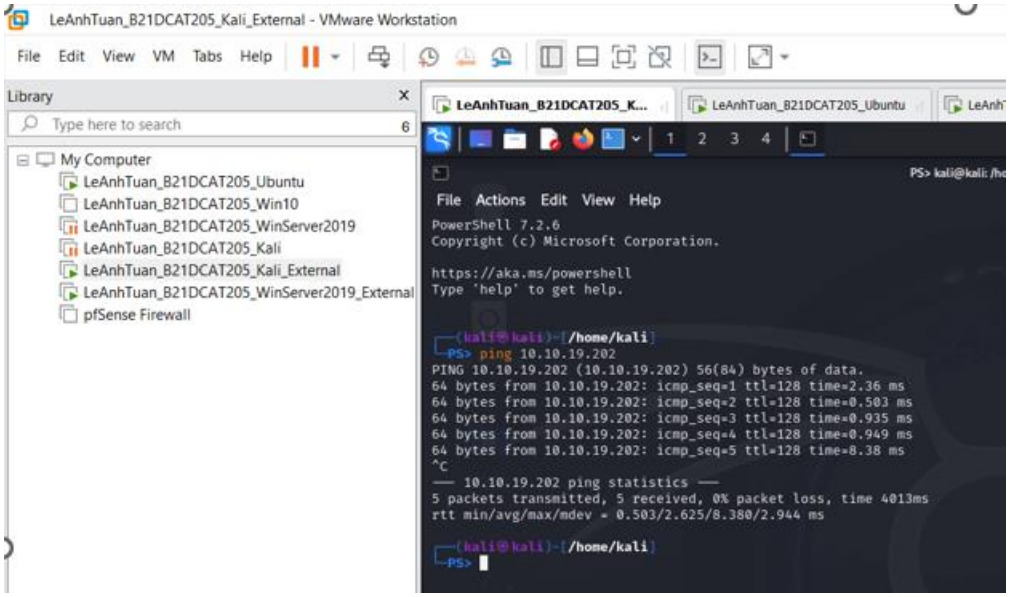


Hình 12: Ping máy Ubuntu internal với Kali internal và Windows Server 2019 internal

Các máy trong external ping cho nhau

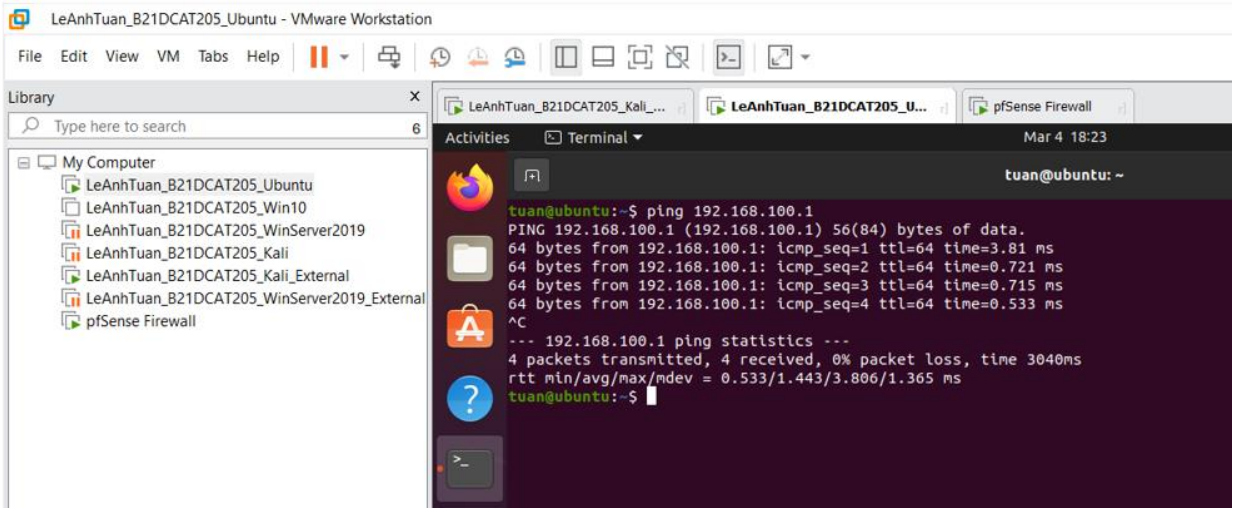


Hình 13: Ping máy Windows Server 2019 external với máy Kali External

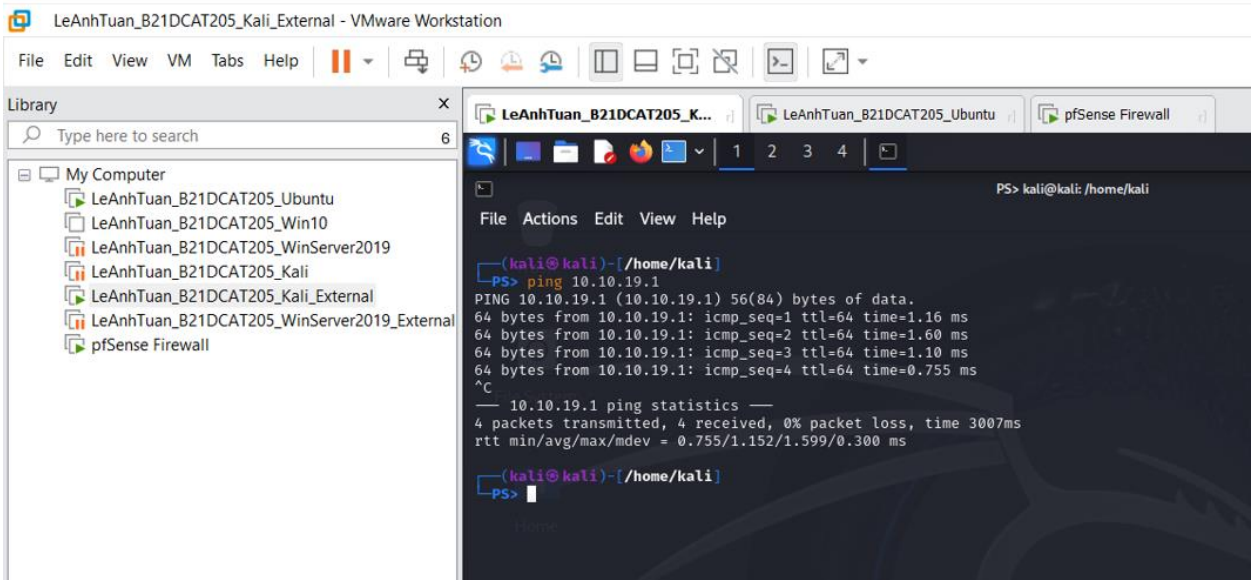


Hình 14: Ping máy Kali External với máy Windows Server 2019 External

Ping thử các máy đến pfsense

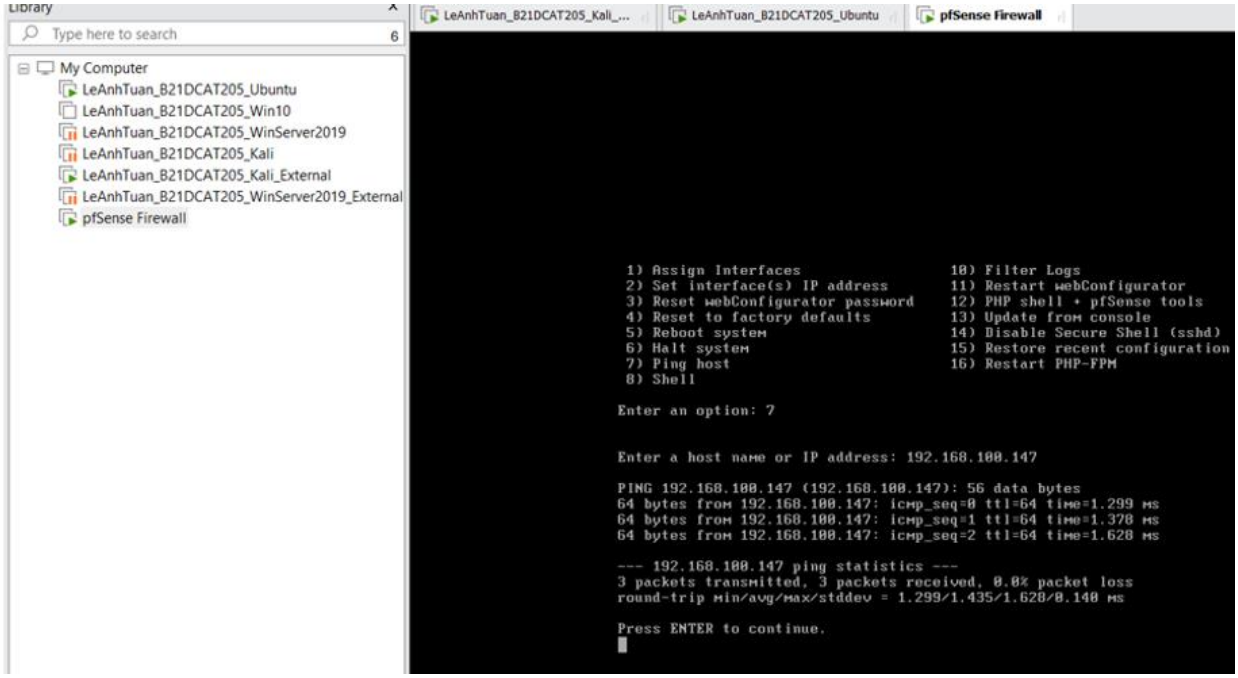


Hình 15: Máy ubuntu internal ping đến máy pfSense

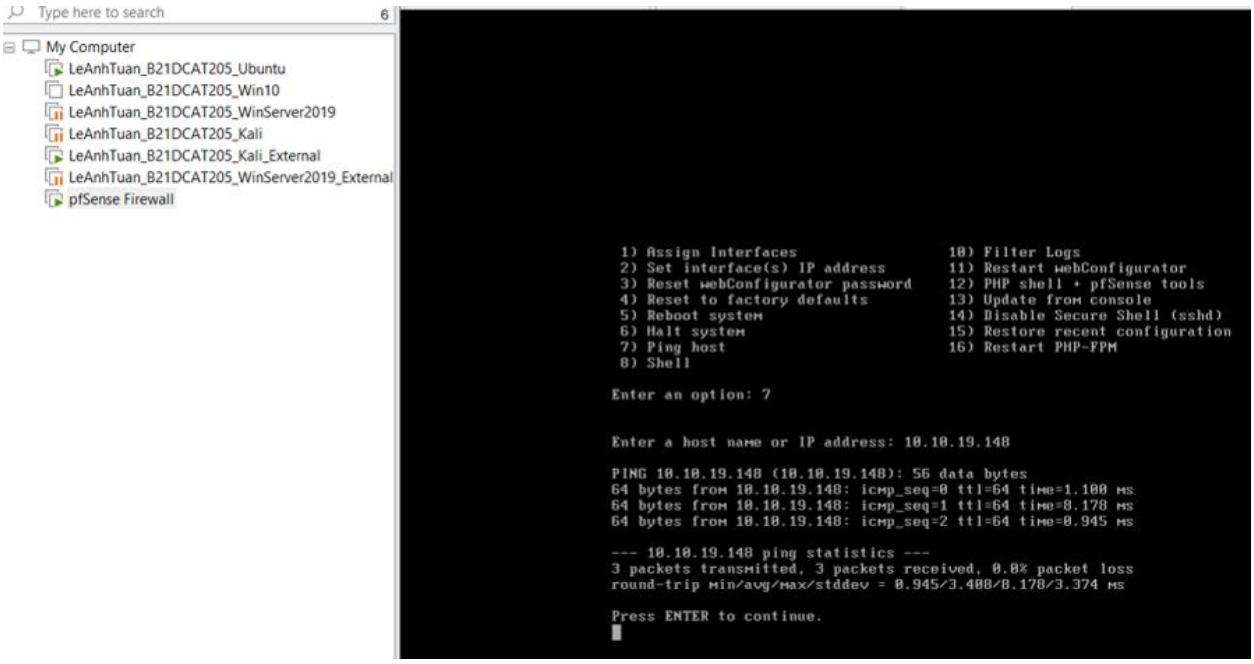


Hình 16: : Máy kali External ping đến máy pfSense

Từ máy pfsense ping đến các máy khác



Hình 17: Máy pfSense ping tới máy ubuntu internal

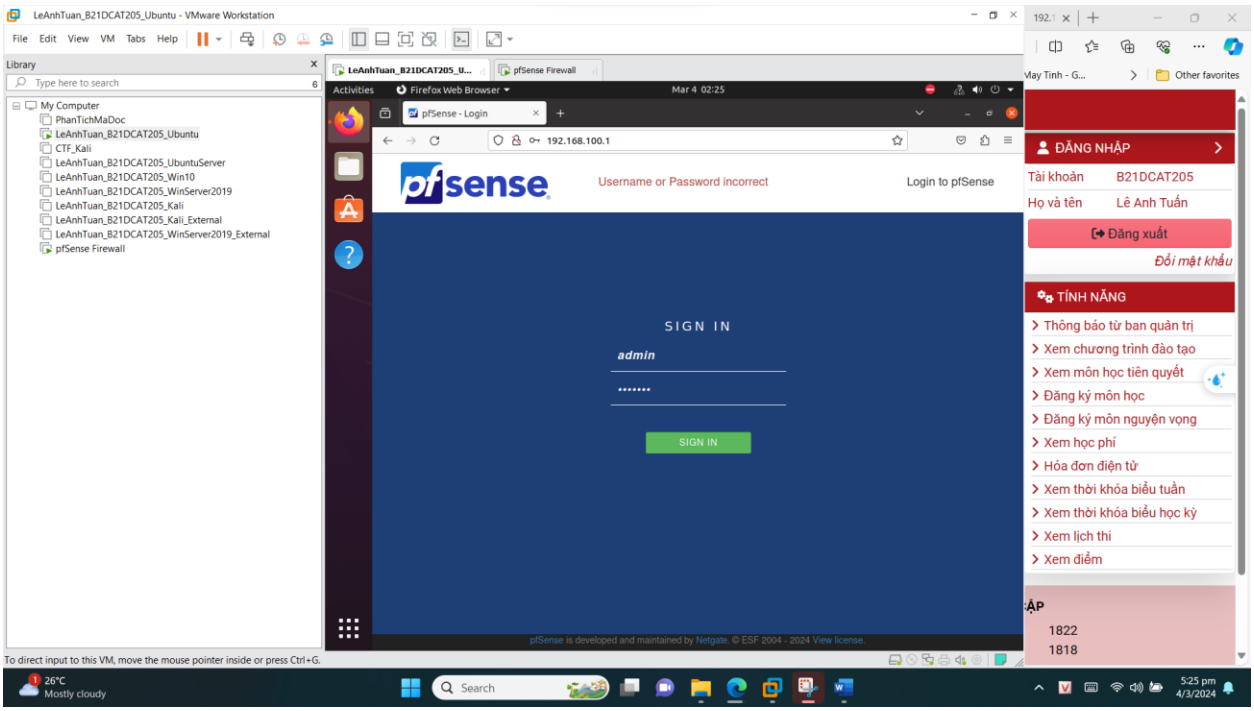


Hình 18: Máy pfSense ping tới máy kali External

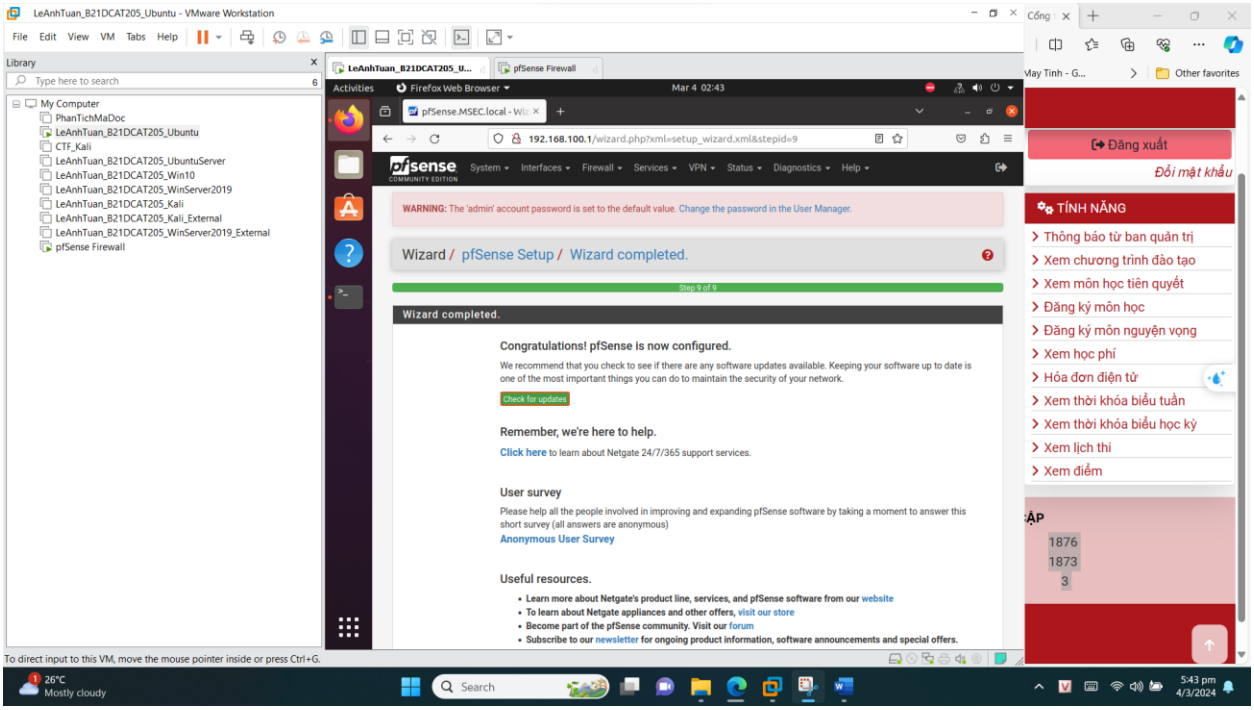
2.2.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình pfsense qua giao diện web.

Đăng nhập với **username: admin** & **passwork: pfsense**



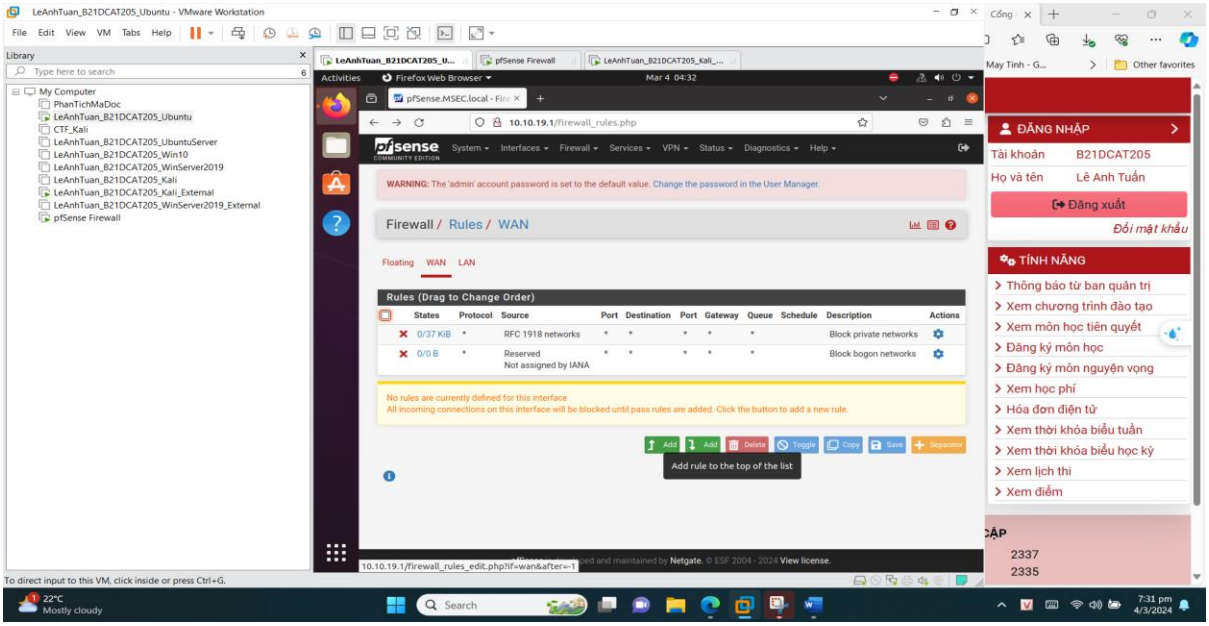
Hình 19:Đăng nhập tại http://192.168.100.1 ở máy Ubuntu internal



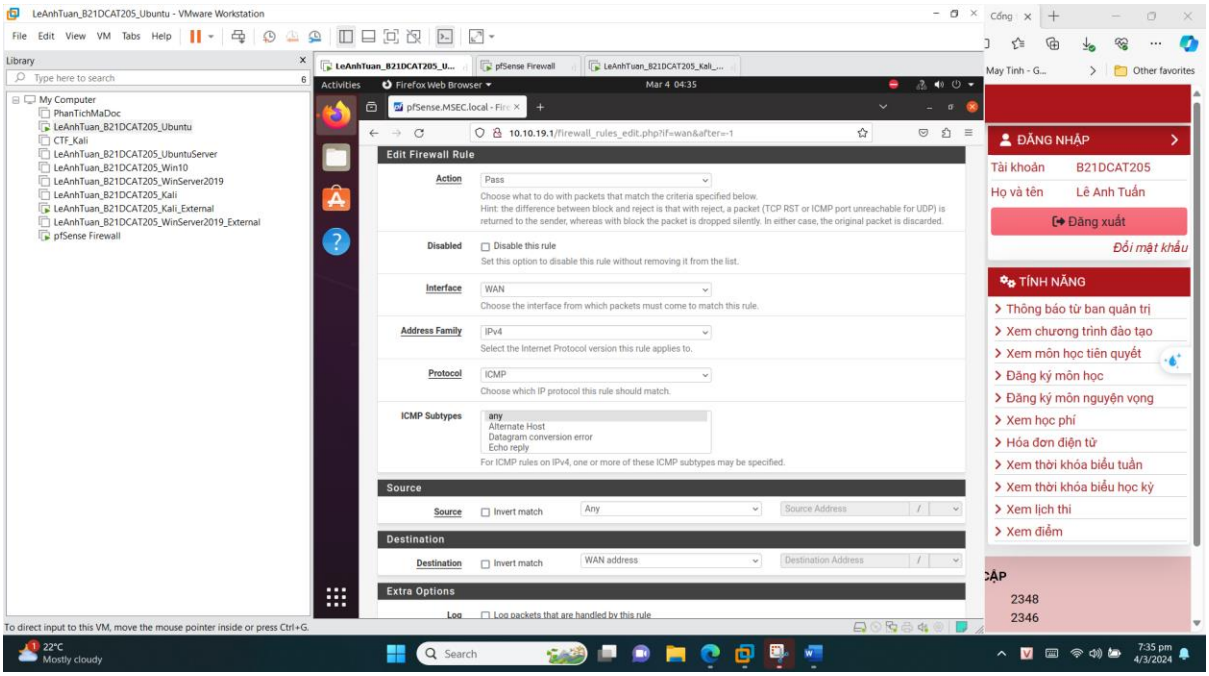
Hình 20: Cấu hình thành công pfsense qua giao diện web.

Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1

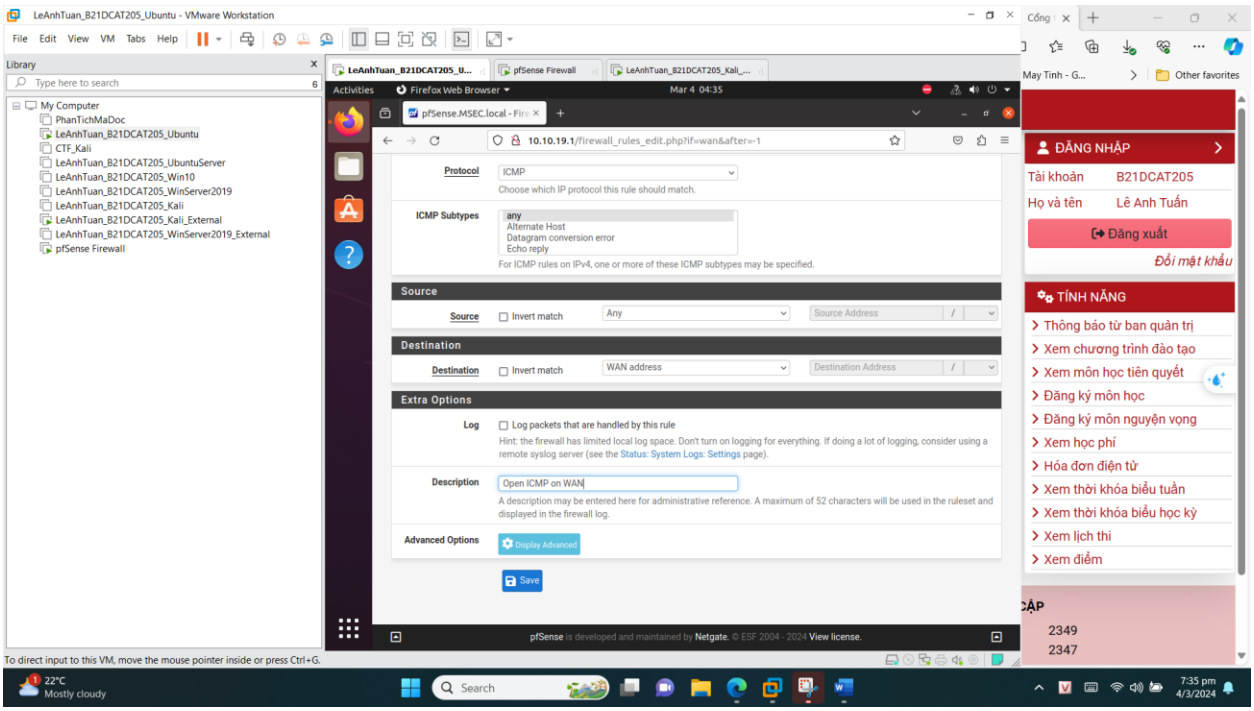
Tại FireWall trên thanh công cụ, chọn Rules.Sau đó nhấn Add để thêm luật



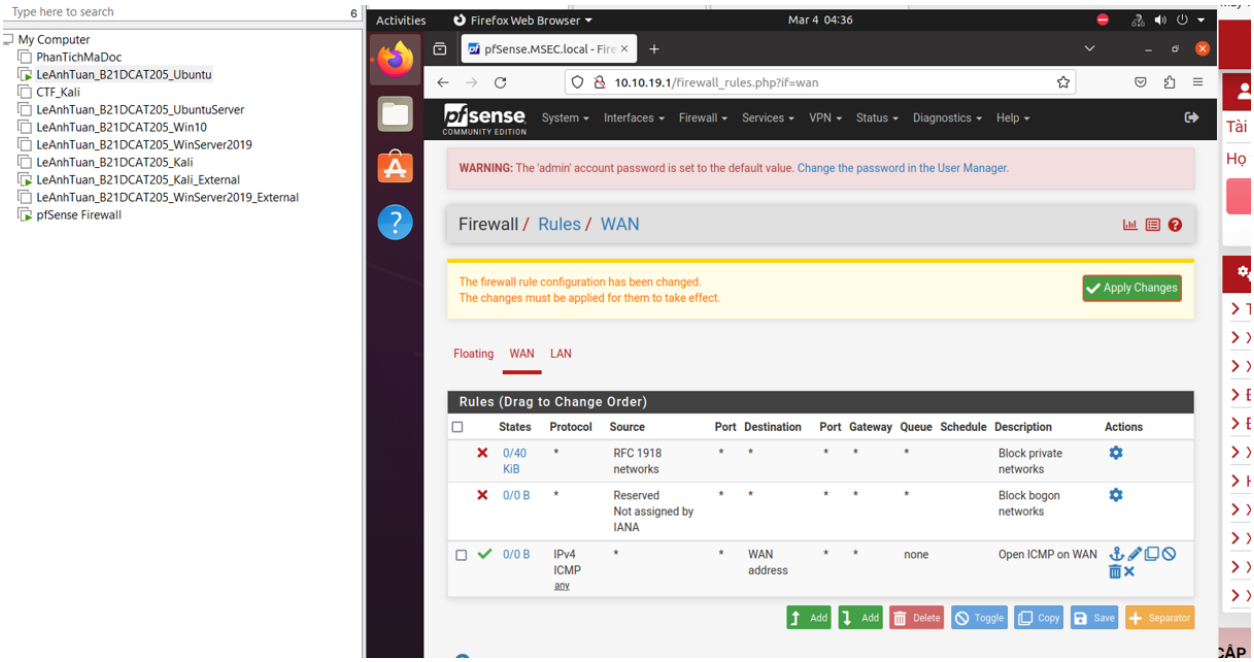
Hình 21: Ấn Add để thêm luật



Hình 22: Cấu hình cho Rules (ảnh 1)

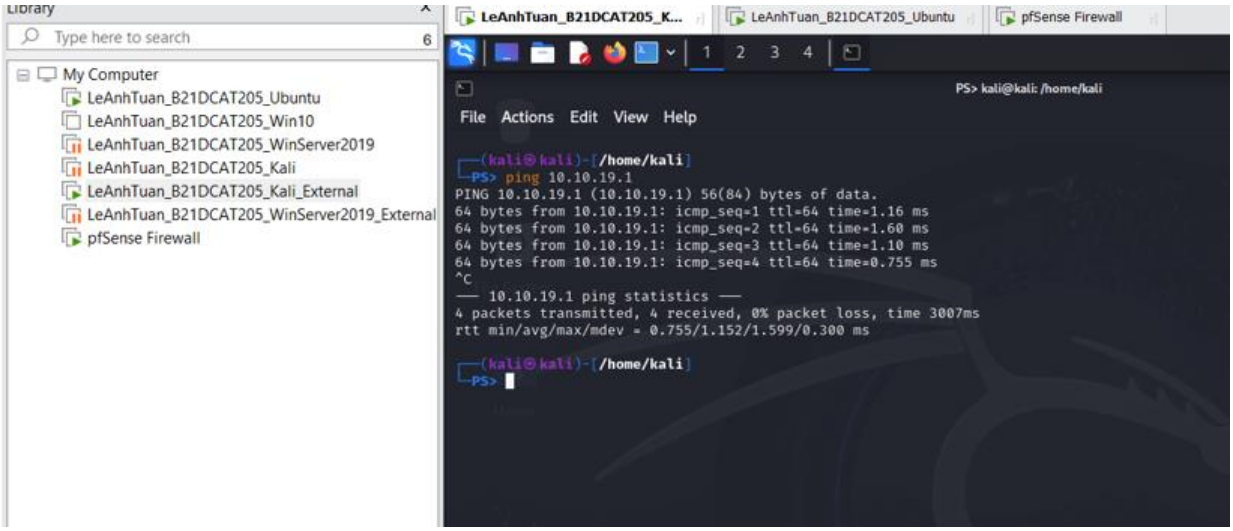


Hình 23: Cấu hình Rules (ảnh 2)



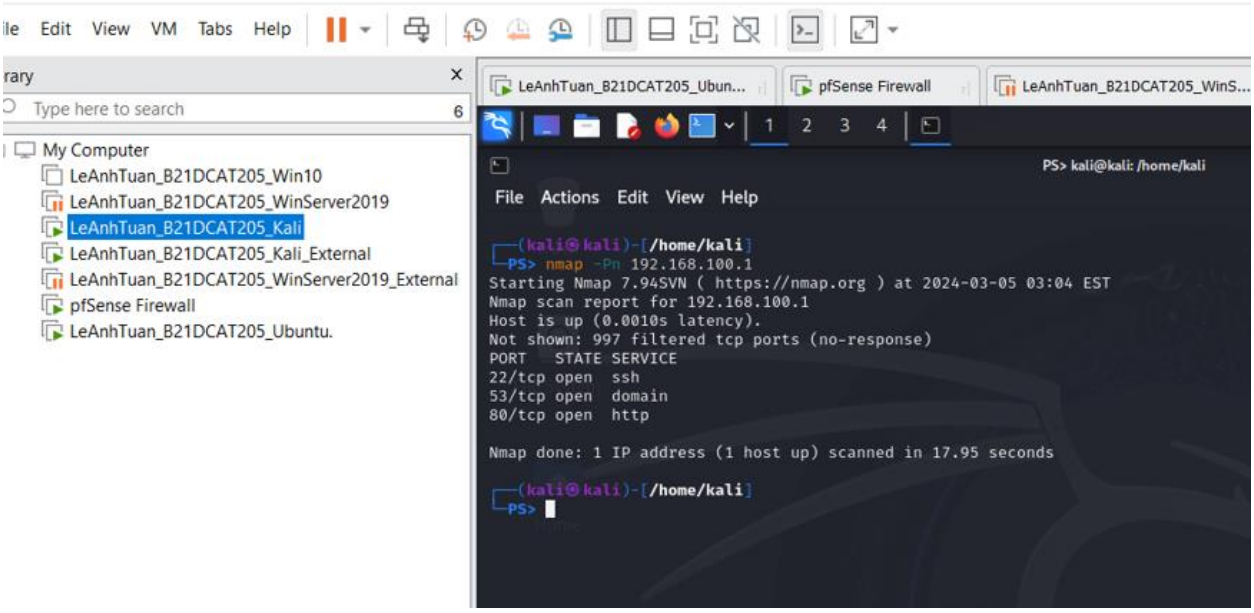
Hình 24: Ấn Apply Changes để lưu thay đổi

Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.

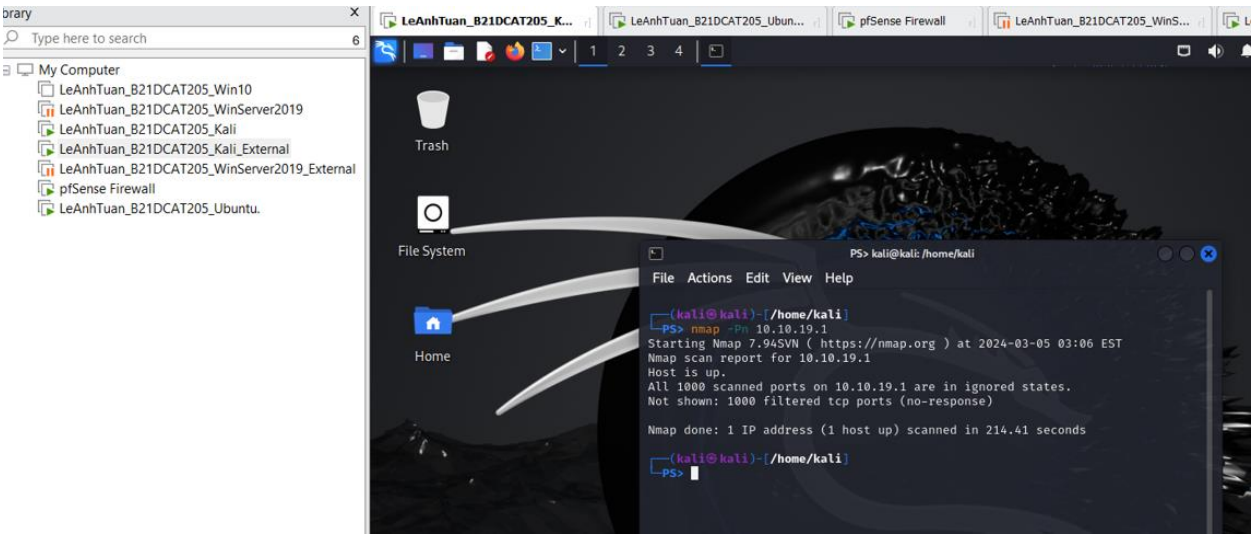


Hình 25: ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.

Sau khi áp dụng rule, máy Kali Linux External không thể ping tới Ubuntu Internal, nhưng Ubuntu Internal có thể ping tới Kali Linux External.



Hình 26: Quét cổng TCP mặc định mở trên giao diện mạng trong của pfSense



Hình 27: Quét cổng TCP mặc định mở trên giao diện mạng ngoài của pfSense

Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?

- Trong giao diện mạng Internal, theo mặc định có 2 cổng TCP được mở: Cổng 80(HTTP), Cổng 53(domain) (Hình ở trên có thêm cổng SSH là do mình tự mở)

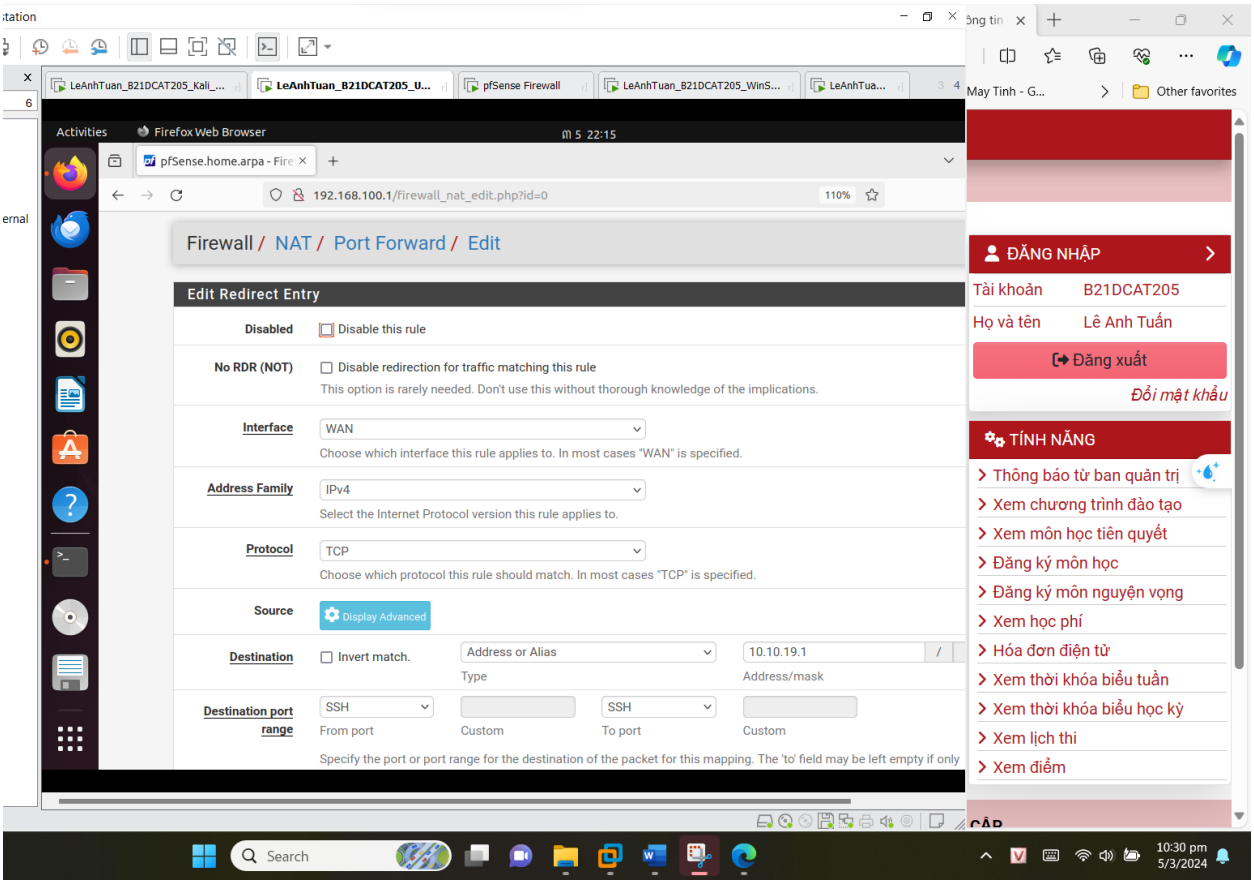
Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng ngoài của pfSense?

- Trong giao diện mạng External không có cổng TCP nào được mở

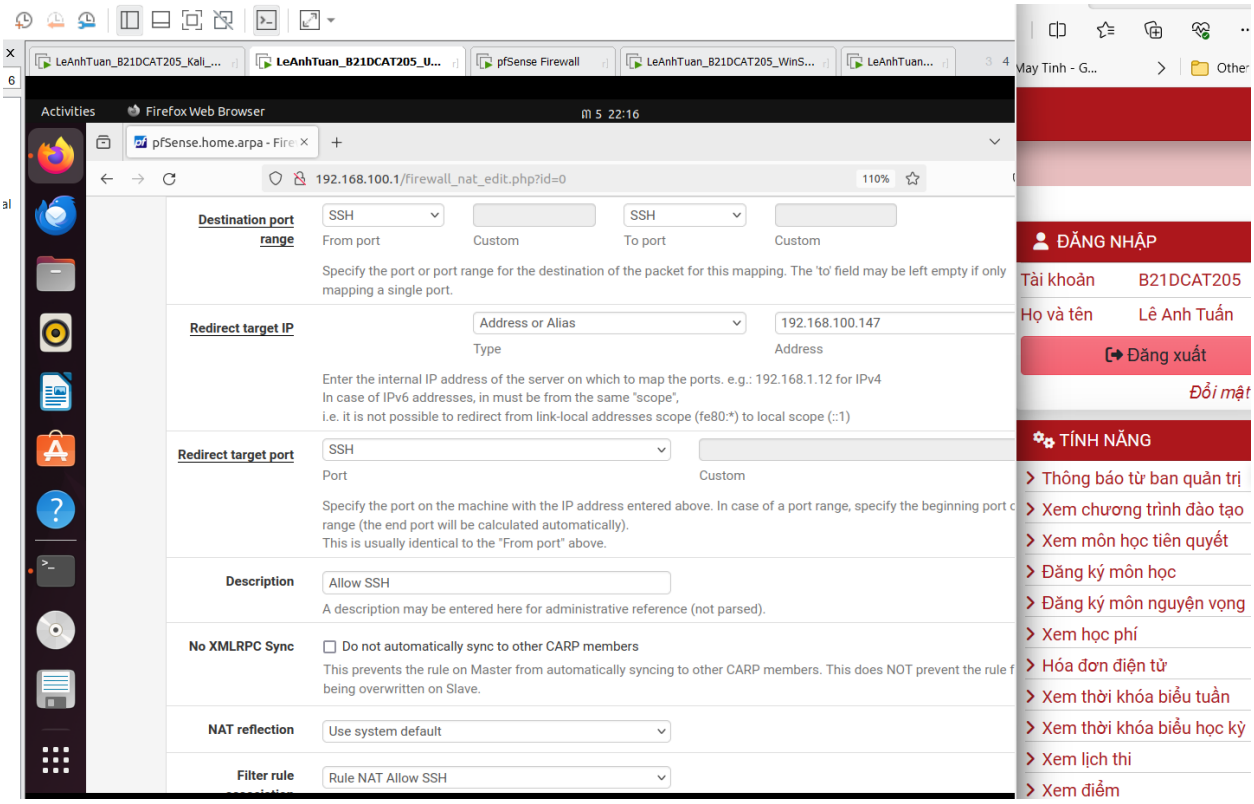
2.2.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web.

Cấu hình cho phép cổng SSH trên IP 192.168.100.147 (Máy Linux victim mạng Internal) được truy cập từ bên ngoài thông qua port forwarding. Nghĩa là khi các máy khách từ mạng 10.10.19.0/24 kết nối với địa chỉ IP của tường lửa pfSense của 10.10.19.1, chúng sẽ được chuyển hướng đến máy Linux victim trong mạng Internal.

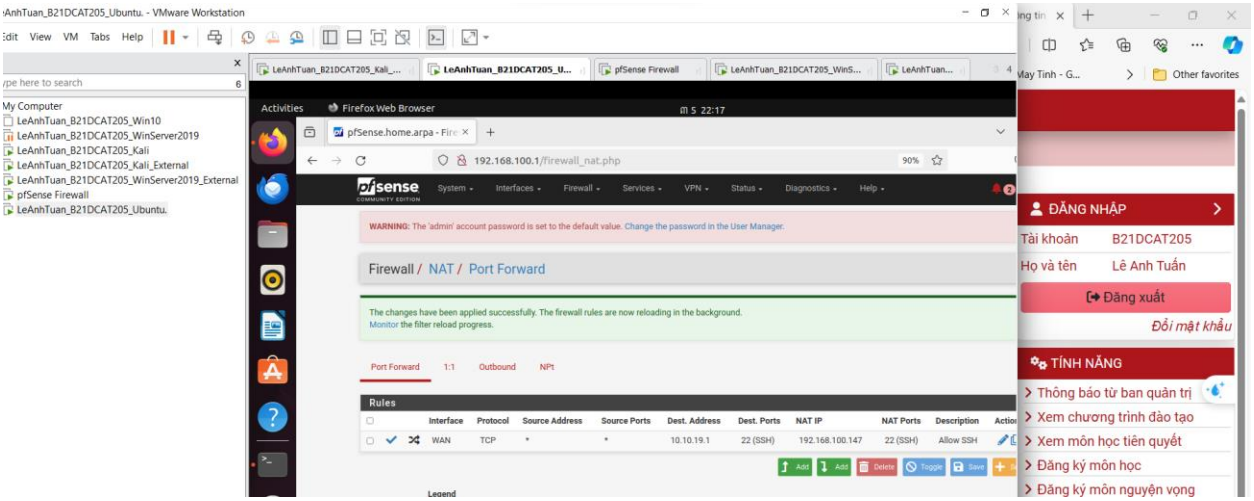


Hình 28: Cấu hình Port Forward (ảnh 1)



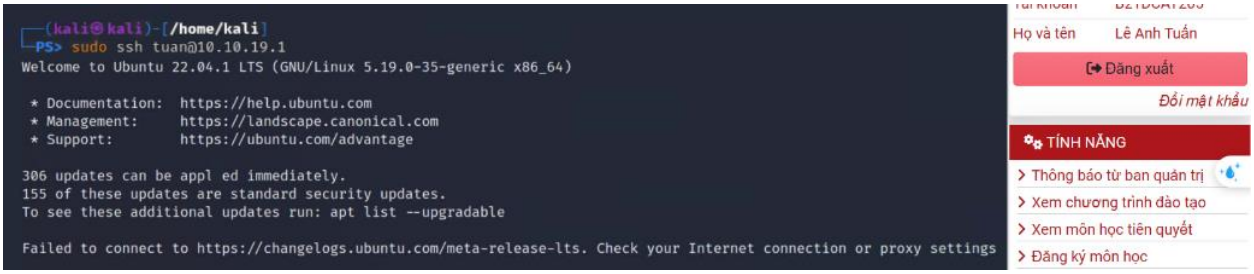
Hình 29: Cấu hình Port Forward (ảnh 2)

Bấm Save để hoàn thành



Hình 30: Cấu hình hoàn tất

Kiểm tra bằng cách truy cập ssh tới 10.10.19.1



Hình 31: SSH thành công từ máy Kali external tới Ubuntu internal

3 Kết luận

- Xây dựng topo mạng và cài đặt, cấu hình địa chỉ IP thành công, các máy trong mạng ping được nhau
- Cài đặt, cấu hình thành công ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal.
- Cài đặt thành công cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal.

4 Tài liệu tham khảo

- VMware Workstation Networking | Mastering VMware
- ducnc/vmware-workstation-network (github.com)
- VirtualBox Network Settings: All You Need to Know (nakivo.com)
- [Network] Giới thiệu về PfSense (viblo.asia)
- Lab 7 pfsense firewall của CSSIA CompTIA Security+®
- Advances Penetration Testing for Highly-Secured Environments Second Edition