**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 5**

**Tìm hiểu và cài đặt, cấu hình tường lửa cho mạng**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 3/2023

I/ 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.

II/ Nội dung thực hành

1. Nội dung lý thuyết

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 đa 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.

1.2 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 như các 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: 1 Aliases 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. Nội dung thực hành Chuẩn bị:

- Phần mềm ảo hóa VMWare

- Các máy ảo máy trạm, máy chủ Windows và Linux

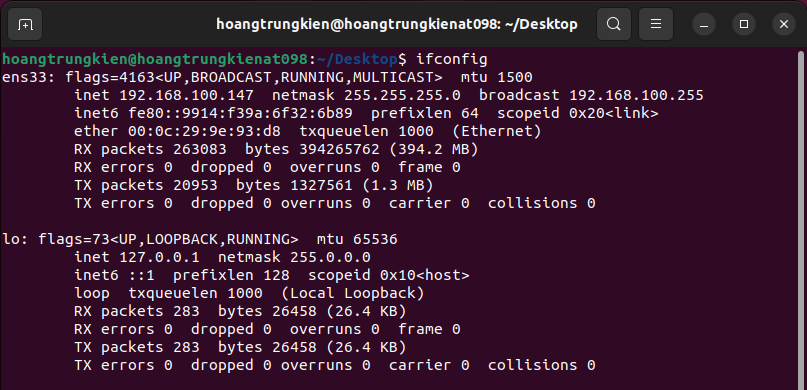
- Tường lửa Pfsense

2.1 Cấu hình topo mạng:

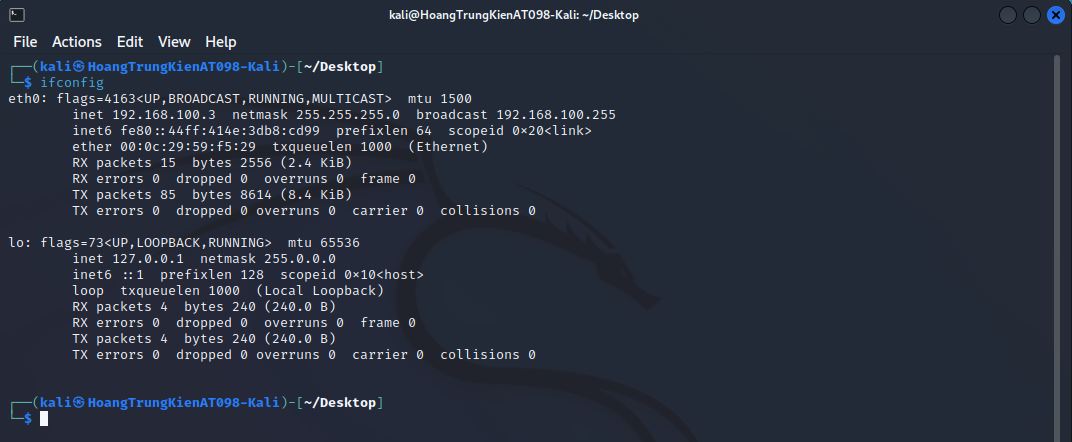
a) Cài đặt và cấu hình hệ thống theo topo mạng:

- Trong mạng Internal

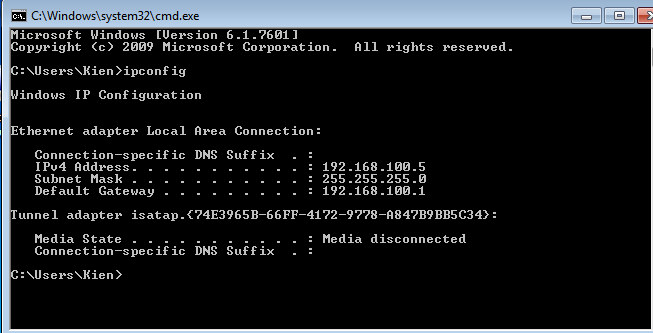
+Cài đặt IP tĩnh cho máy Linux Victim Internal:



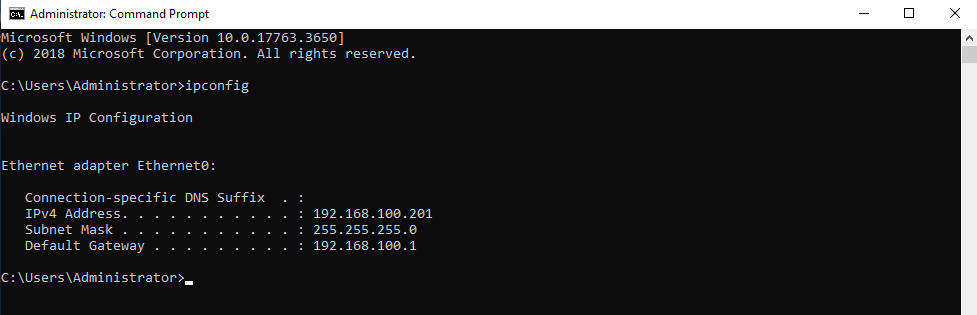
+Cài đặt IP tĩnh cho máy Kali Attack Internal:



-Cài đặt IP tĩnh cho máy Windows Attack Internal

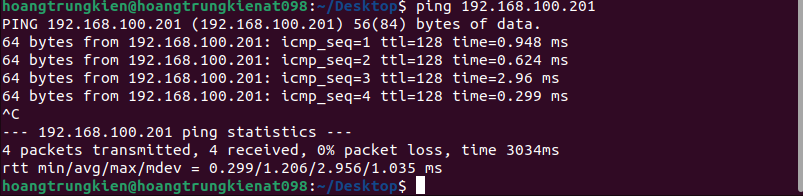


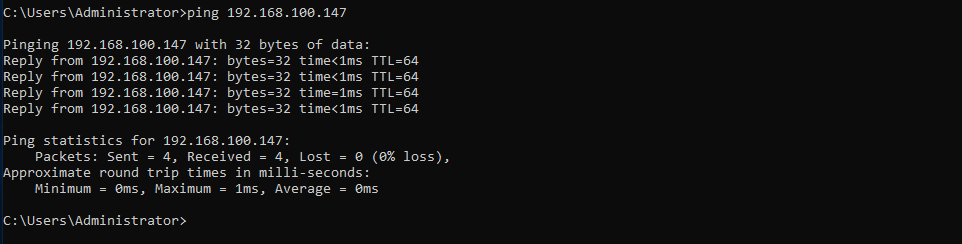
-Cài đặt IP tĩnh cho máy Windows Server Victim Internal:



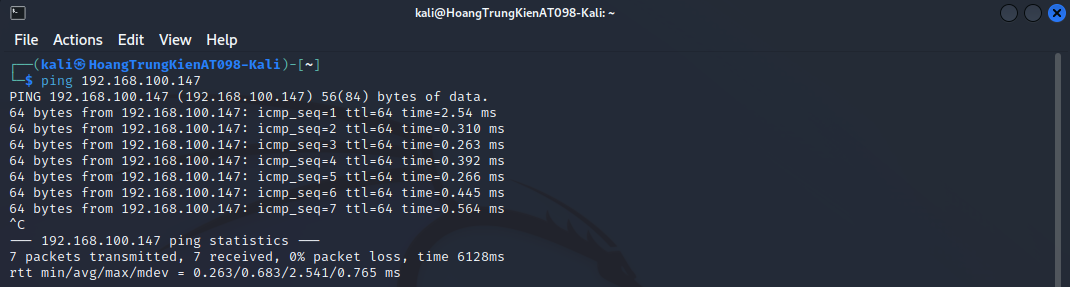
Kiểm tra các mạng trong Internal đã thông với nhau:

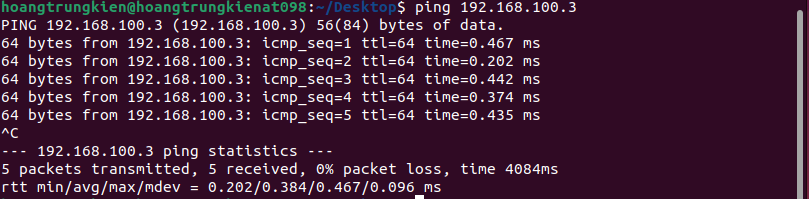
+Linux Victim Internal với Windows Server Victim Internal:



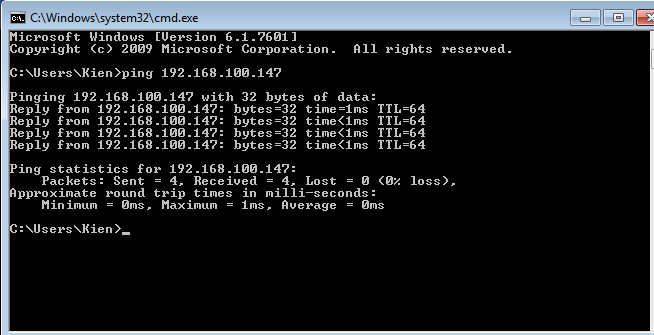


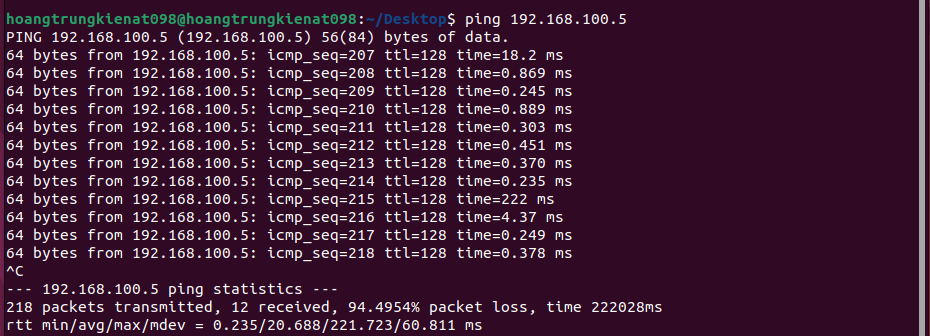
+Linux Victim Internal với Kali Attack Internal:



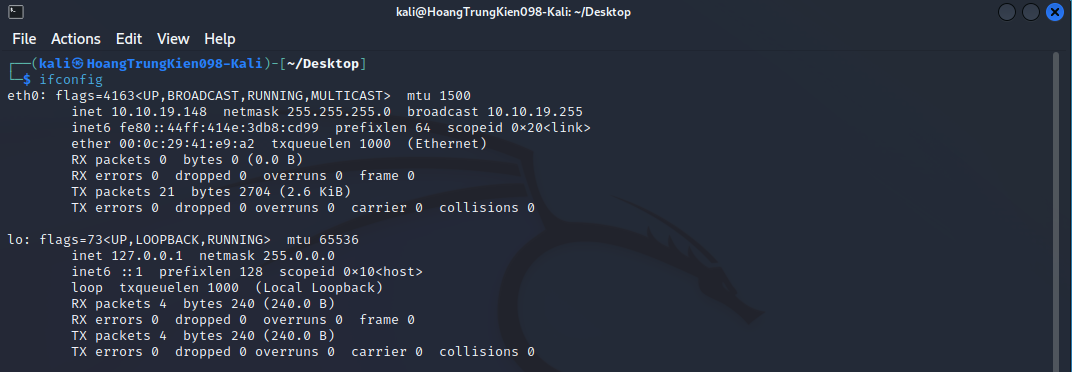


+ Linux Victim Internal với Windows Attack Internal

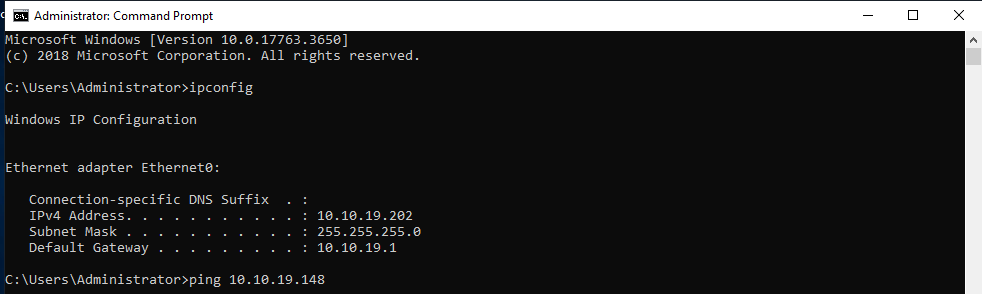




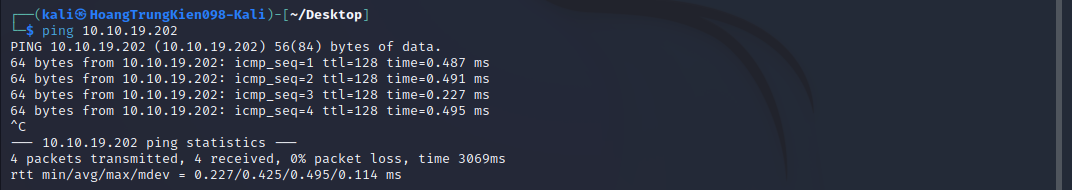
- Trong mạng External

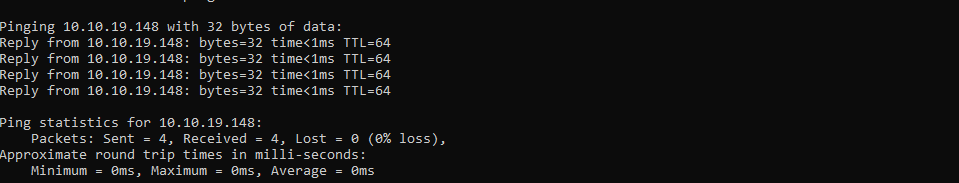
Cài đặt IP tĩnh cho máy Kali Attack External tương tự như trong phần Internal→  Kiểm tra địa chỉ IP 

Cài đặt IP tĩnh cho máy Windows Server Victim External tương tự như trong phần Internal→  Kiểm tra lại địa chỉ IP



Kiểm tra các mạng trong External đã thông với nhau:

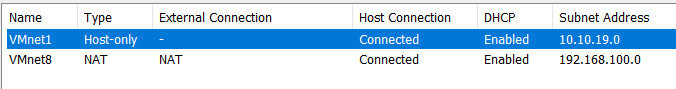


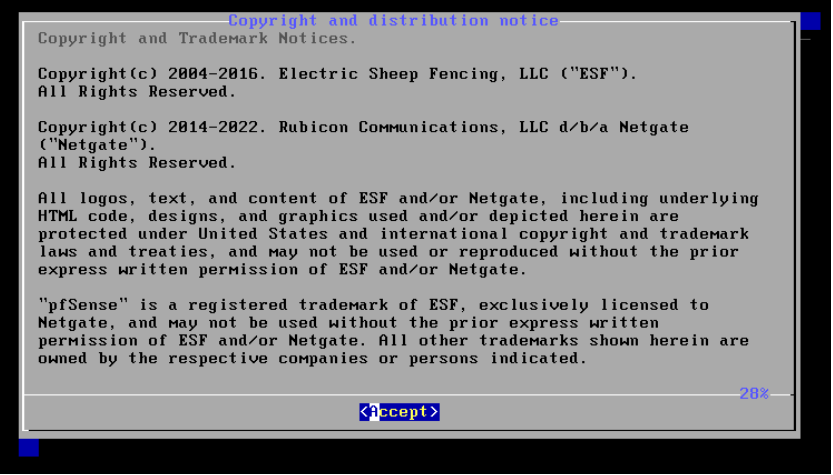


2.2 Cài đặt cấu hình pfsense firewall cho lưu lượng mạng ICMP

- Cài đặt Pfsense.

Trong Vmware, tạo thêm một Network Adapter:





Xét thành công địa chỉ

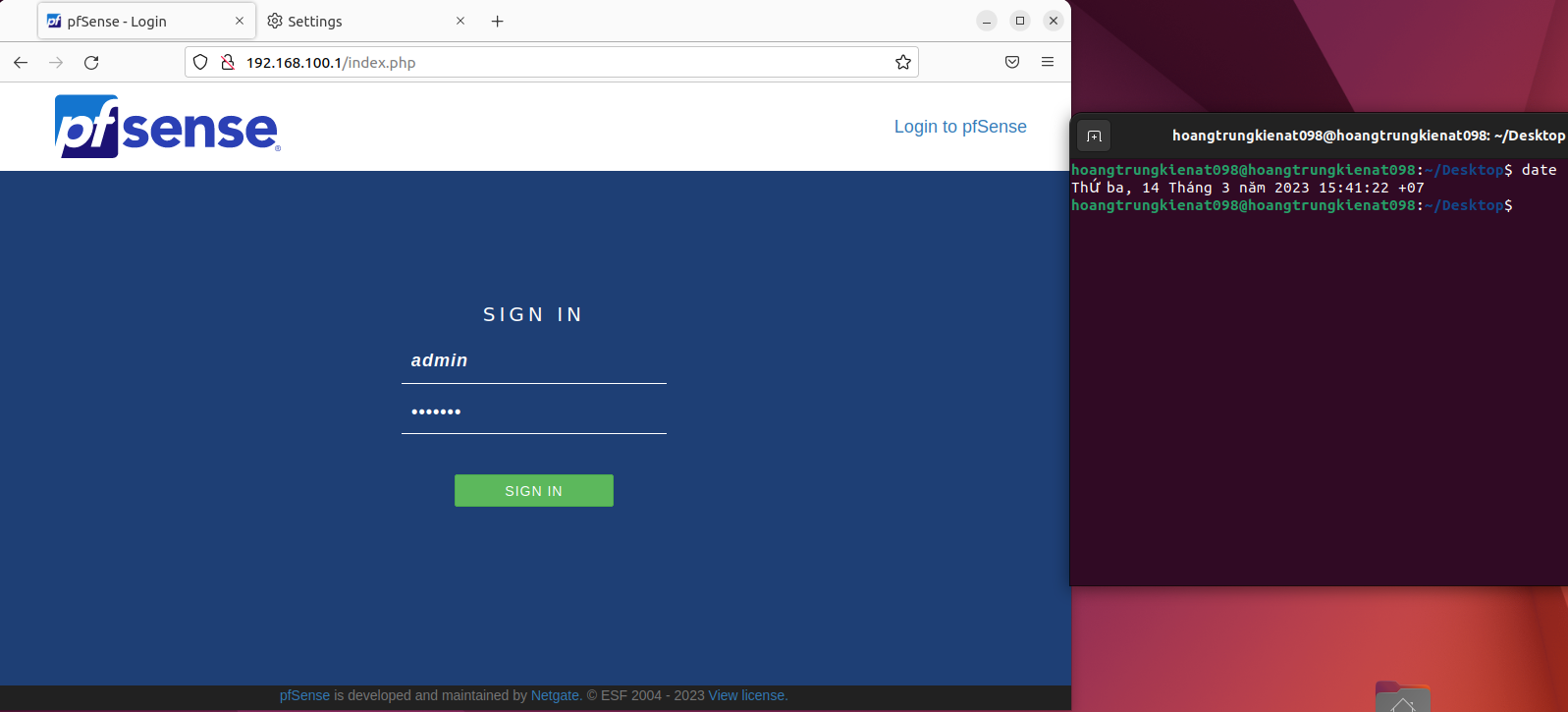


  → Chọn accept

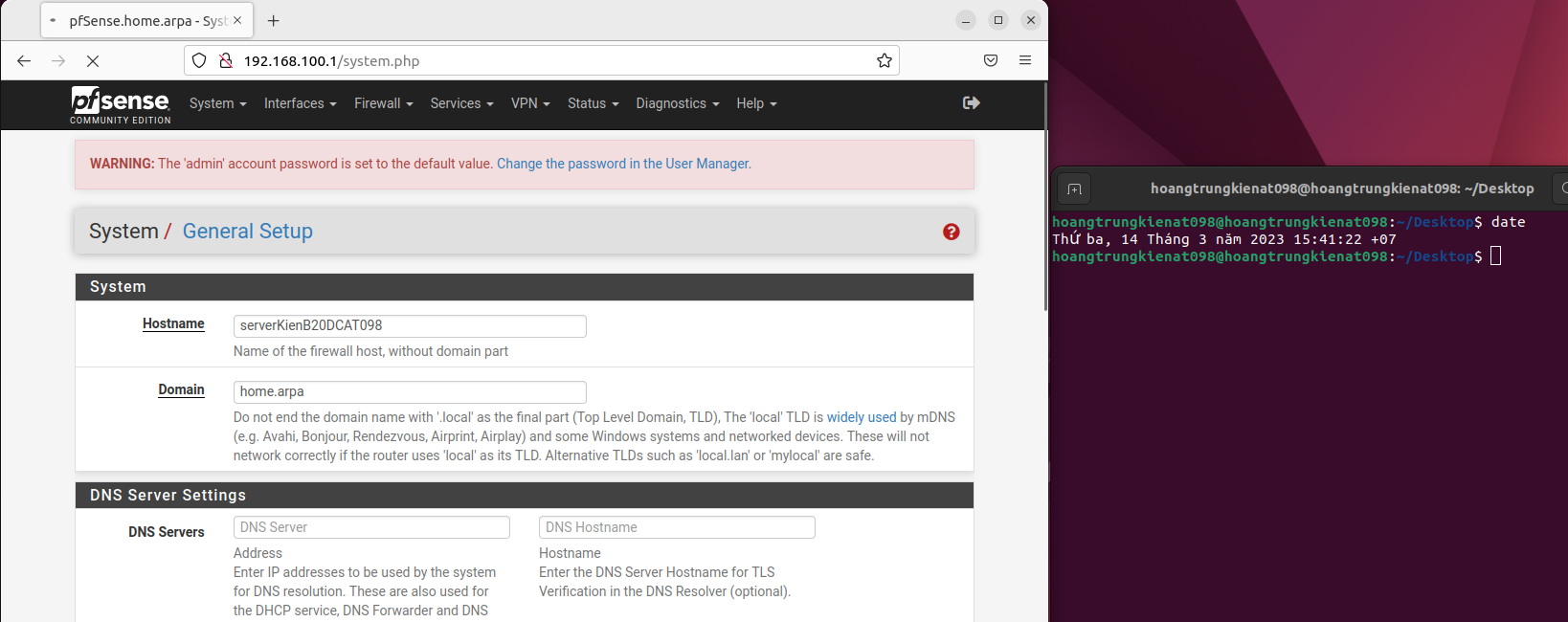
Các bước tiếp theo để mặc định, thực hiện cấu hình Pfsense ta được:

Dùng máy Ubuntu Victim Internal truy cập vào địa chỉ 192.168.100.1

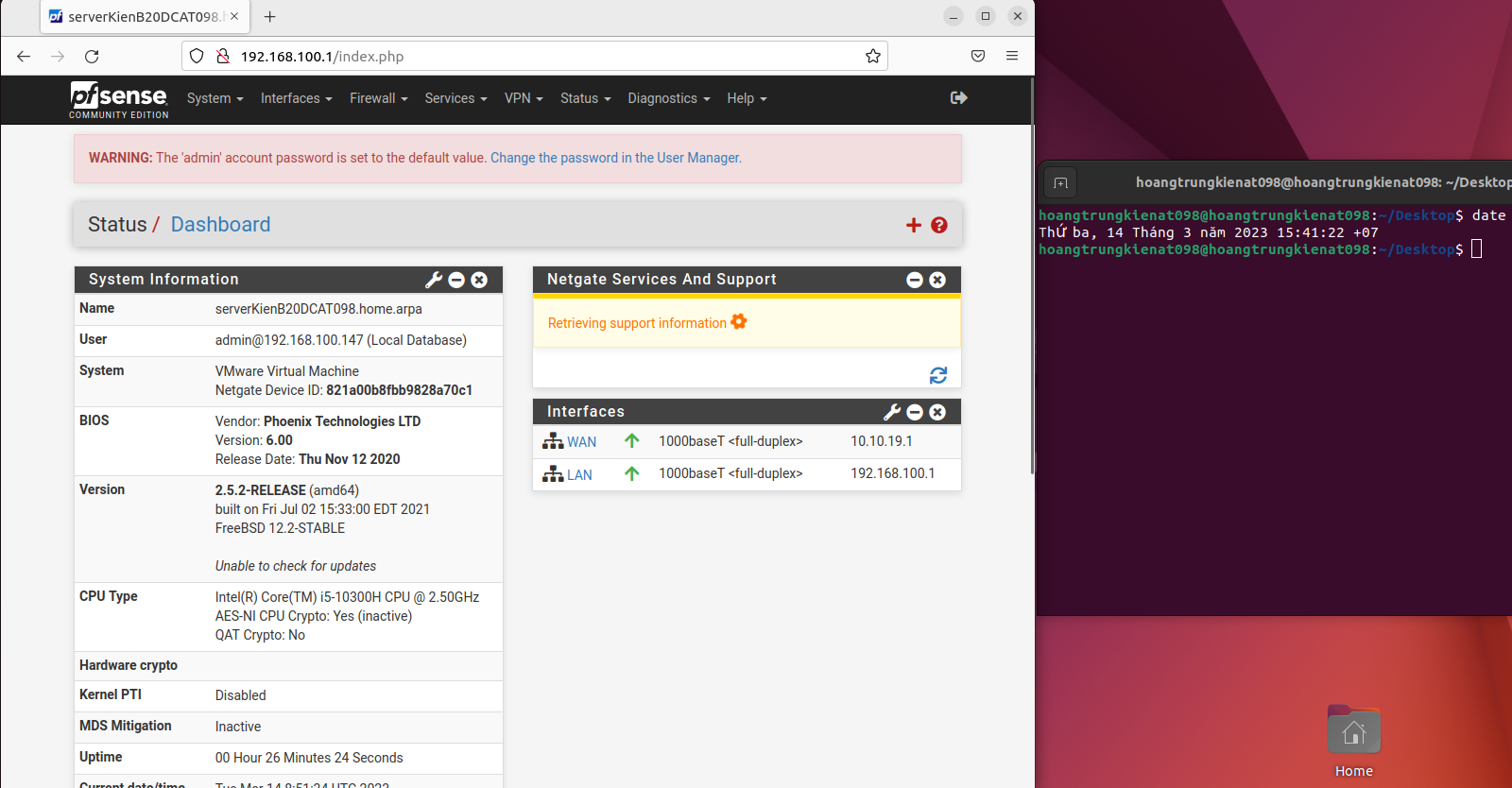
Đăng nhập tài khoản/mật khẩu là: admin/pfsense



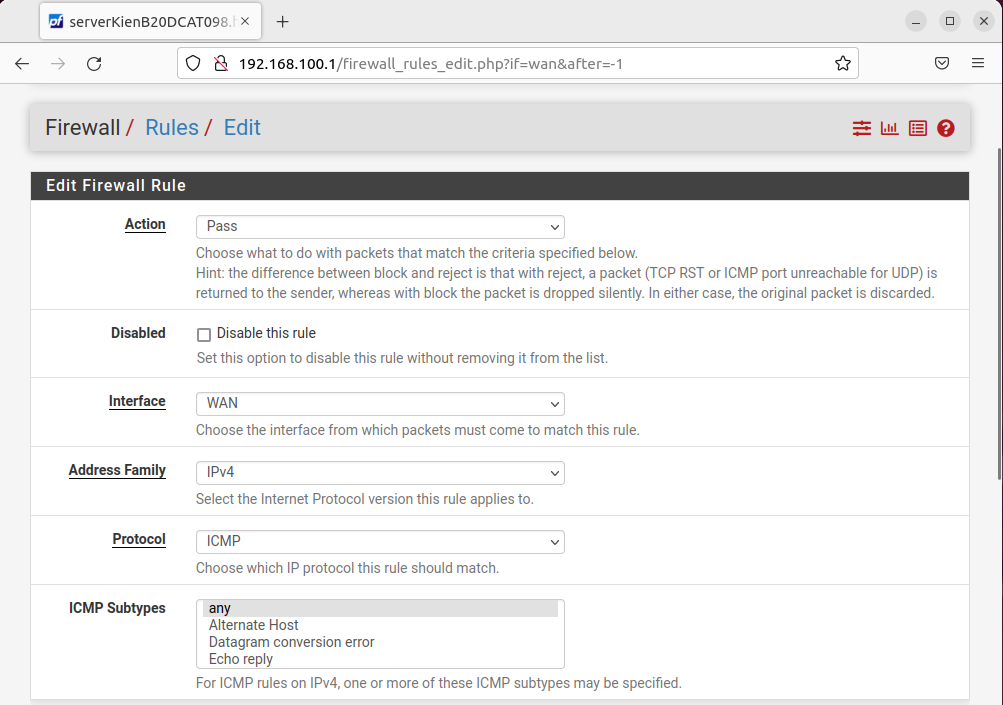
Sau khi đăng nhập thành công, thực hiện cài đặt mặc định chọn Next.

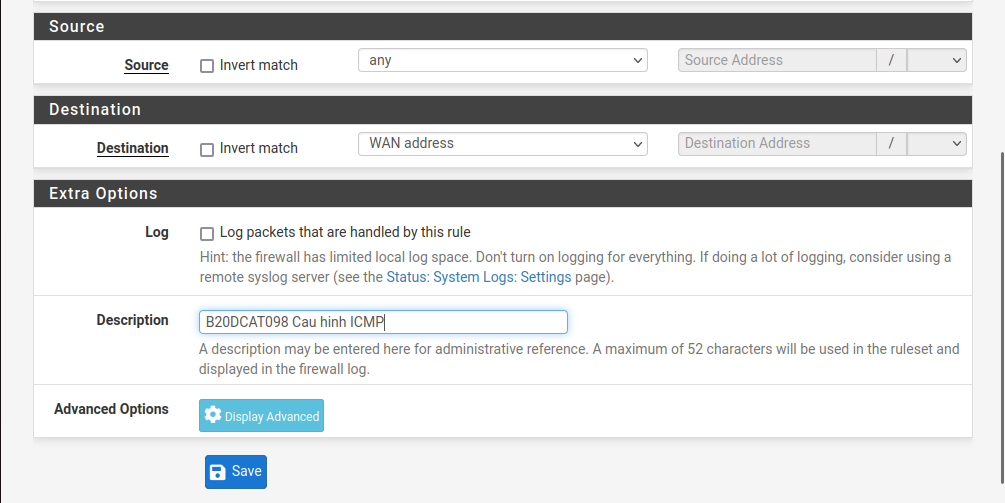


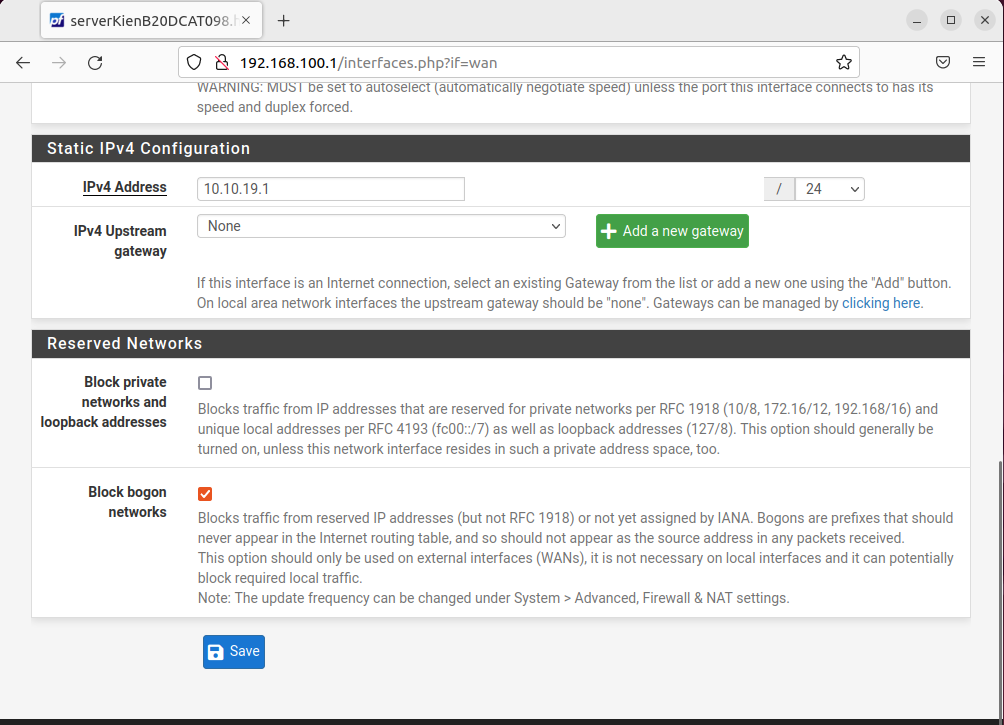
Thu được kết quả như sau:



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

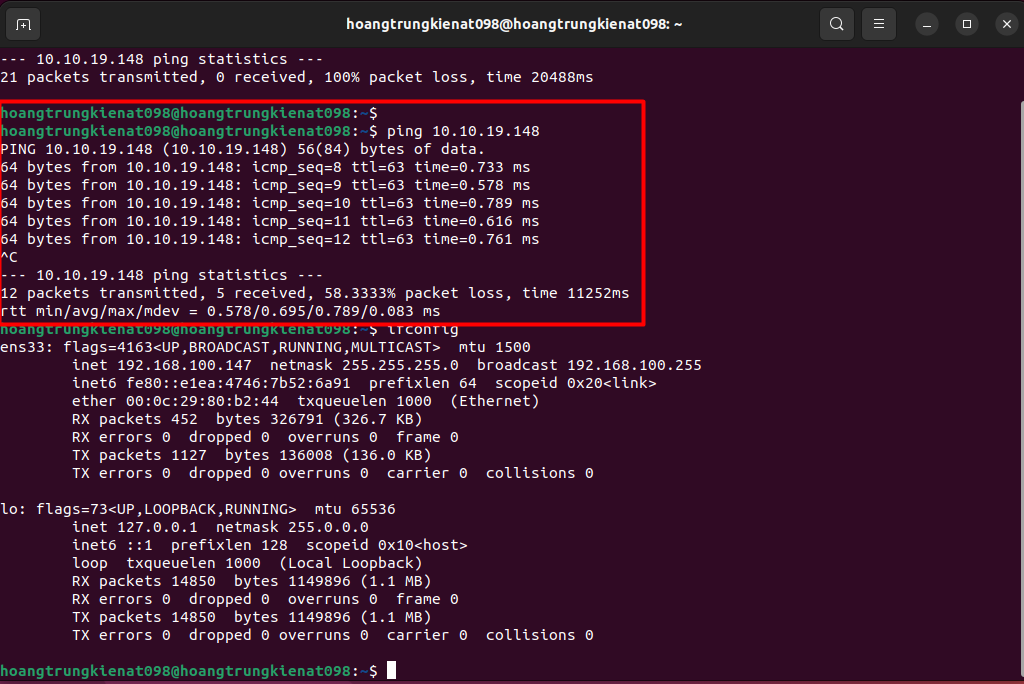


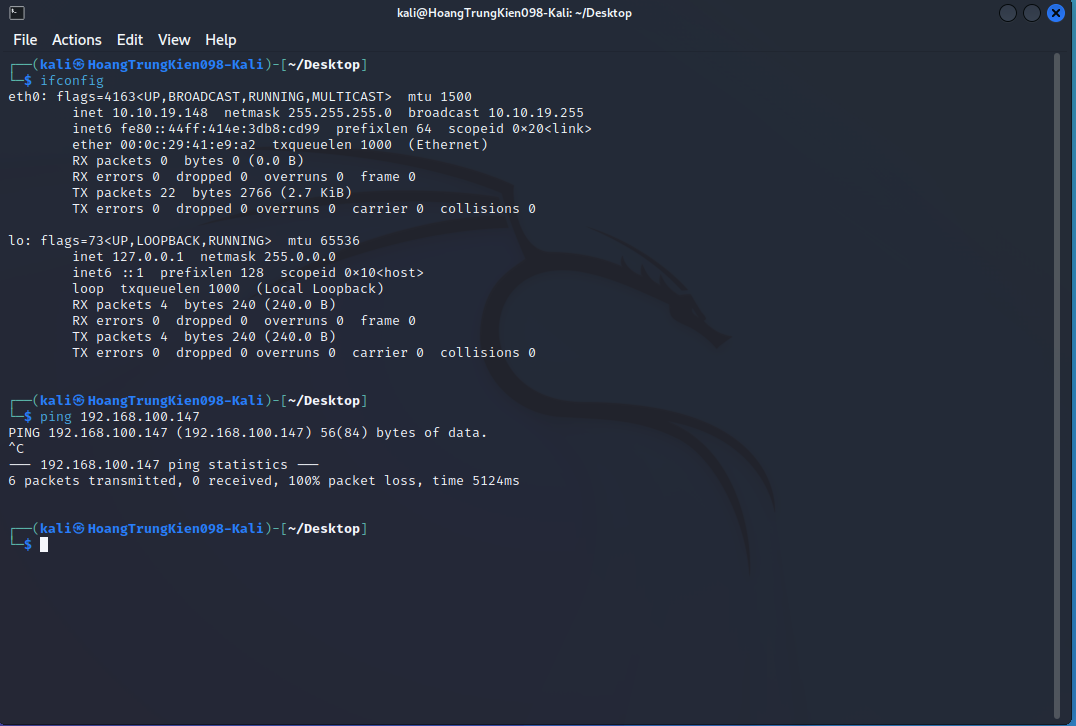




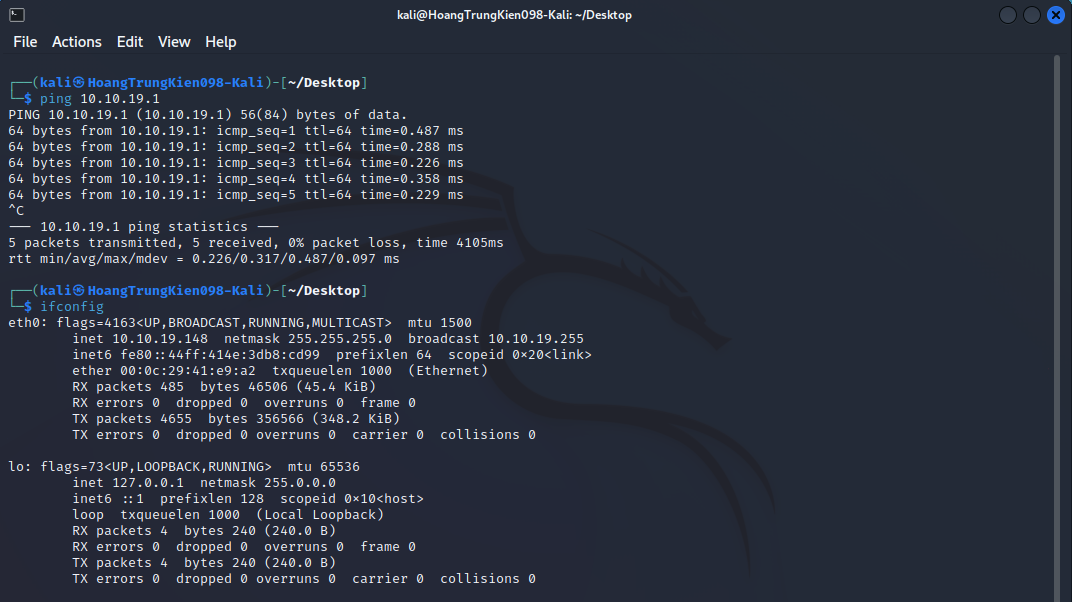
- Kiểm tra kết quả:

+ Các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal.

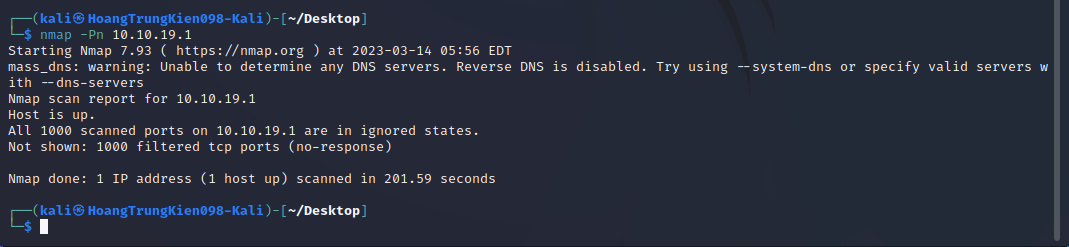




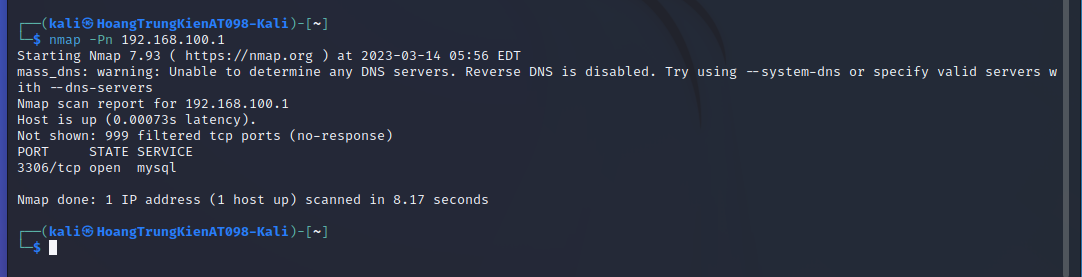
+ Máy Kali attack ở mạng ngoài ping tới 10.10.19.1



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

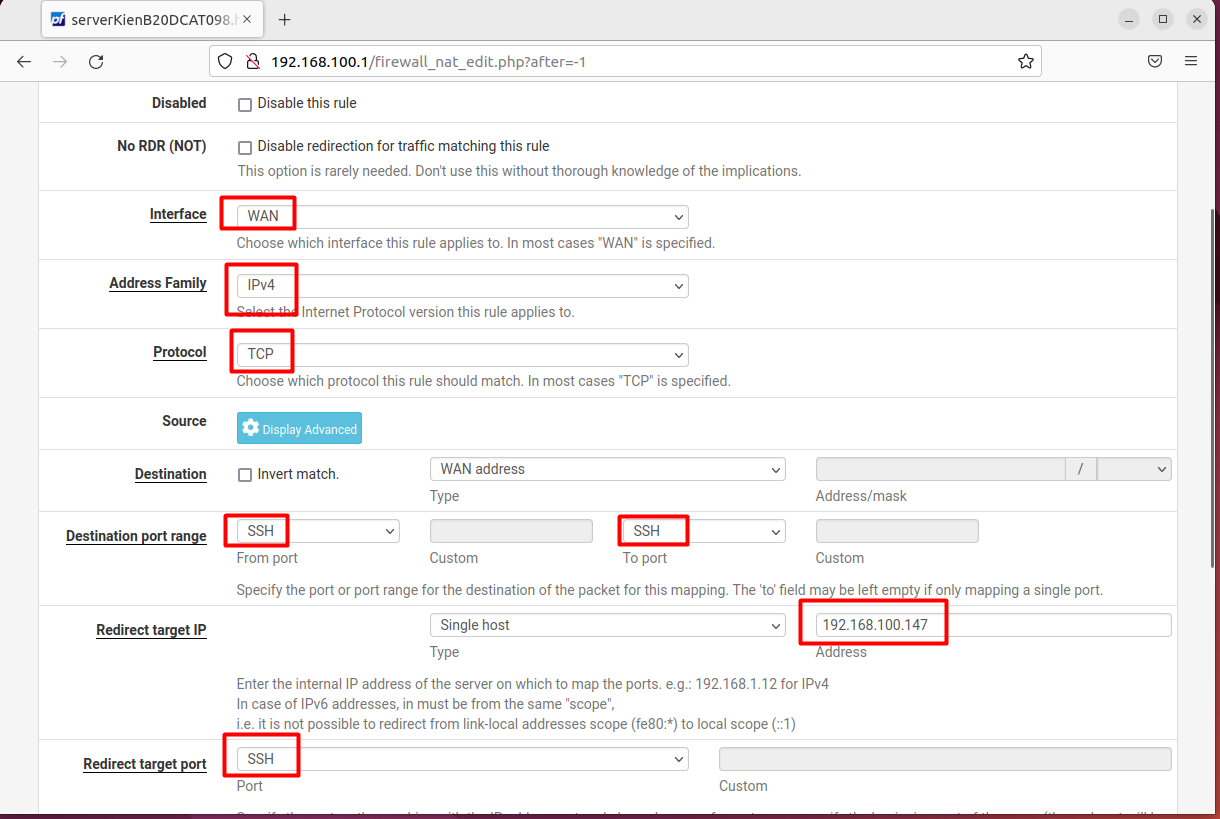


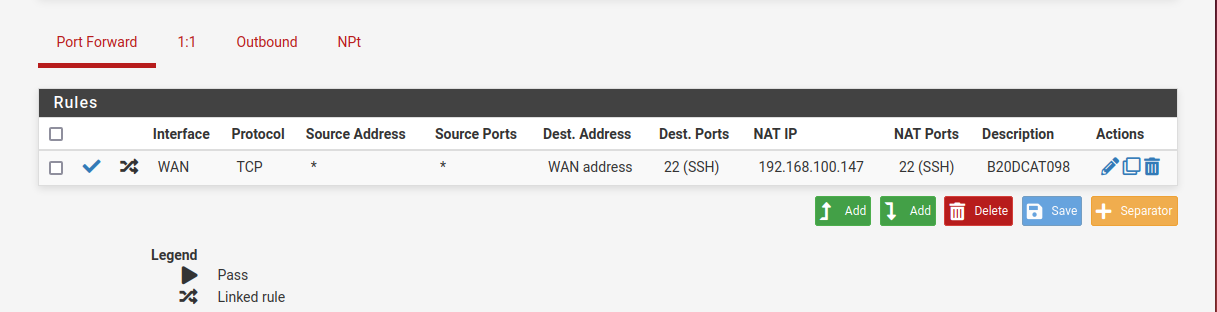
Quét cổng TCP mặc định mở trên giao diện mạng trong của pfSense



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.





**Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?**

