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

**KHOA AN TOÀN THÔNG TIN**

****

**BÁO CÁO BÀI THỰC HÀNH**

**HỌC PHẦN: THỰC TẬP CƠ SỞ**

**MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 2.1**

**CÀI ĐẶT, CẤU HÌNH MẠNG DOANH NGHIỆP VỚI PFSENSE FIREWALL**

Sinh viên thực hiện: Ngô Quang Thắng – B22DCAT287

Giảng viên hướng dẫn: Quản Trọng Thế

**HỌC KỲ 2 NĂM HỌC 2024-2025**

MỤC LỤC

[MỤC LỤC 2](#_Toc193560074)

[CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH 3](#_Toc193560075)

[1.1 Mục đích 3](#_Toc193560076)

[1.2 Tìm hiểu lý thuyết 3](#_Toc193560077)

[**1.21**. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware 3](#_Toc193560078)

[**1.2.2**. Tìm hiểu về Pfsense 7](#_Toc193560079)

[CHƯƠNG 2. NỘI DUNG THỰC HÀNH 11](#_Toc193560080)

[2.1 Chuẩn bị môi trường 11](#_Toc193560081)

[2.2 Các bước thực hiện 11](#_Toc193560082)

[**2.2.1** Cấu hình topo mạng 11](#_Toc193560083)

[**2.2.2** Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP 19](#_Toc193560084)

[**2.2.3** Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal 25](#_Toc193560085)

[TÀI LIỆU THAM KHẢO 29](#_Toc193560086)

1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH
   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

* 1. Tìm hiểu lý thuyết

**1.21**. Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware

VMware Workstation là phần mềm ảo hóa trên máy tính, cung cấp khả năng chạy và mô phỏng nhiều hệ điều hành trên một máy tính vật lý. Wmware Workstation đi kèm - nhiều tính năng kết nối mạng giúp bạn tạo và quản lý mạng riêng, chia sẻ hoặc cách ly mạng bên trong Vmware.

Để có thể sử dụng phần mềm này hiệu quả, chúng ta cần phải hiểu về các kết nối mạng, cách thiết lập và cài đặt hệ thống mạng ảo trong phần mềm. Các thành phần hình thành nên mạng ảo trong VMware gồm switch ảo, card mạng ảo, DHCP server ảo và thiết bị NAT.

**a**. Switch ảo (Virtual Switch)

Cũng giống như switch vật lý, một Virtual Switch kết nối các thành phần mạng ảo lại với nhau. Những switch ảo hay còn gọi là mạng ảo, chúng có tên là VMnet0, VMnet1, VMnet2… một số switch ảo được gắn vào mạng một cách mặc định. Mặc định khi ta cài Wmware thì có sẵn 3 Switch ảo như sau:

− VMnet0 chế độ Bridged (cầu nối),

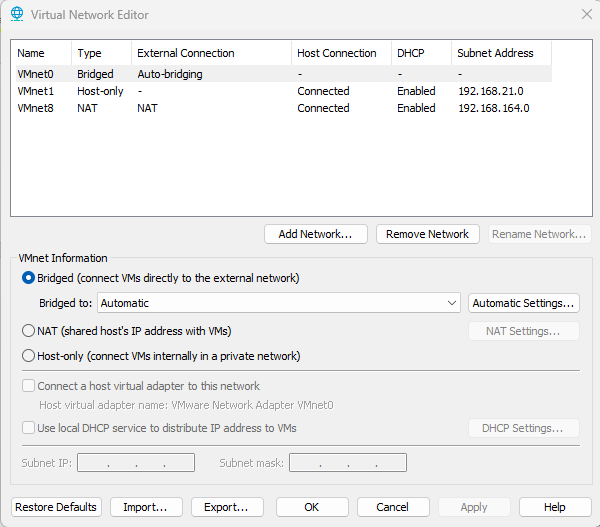
− VMnet8 chế độ NAT

− VMnet1 chế độ Host-only.

Ta có thể thêm, bớt, chỉnh các option của VMnet bằng cách vào menu Edit -> Virtual Network Editor…

VMware Workstation (phiên bản 12) cho phép tạo 20 switch ảo trên Windows và 255 cái trên Linux. Trên mỗi Switch ảo trên Windows thì các kết nối của các máy tính ảo (host) vào mỗi Switch ảo là không giới hạn, còn trên Linux thì 32 máy ảo. Để thêm hoặc bớt VMnet ta có thể chọn Add Network… và Remove Network…

Khi ta tạo các VMnet, thì trên máy thật sẽ tạo ra những card mạng ảo tương ứng với VMnet đó, dùng để kết nối Virtual Switch với máy tính thật, giúp máy thật và máy ảo có thể liên lạc được với nhau. Riêng VMnet0 kết nối trực tiếp với card mạng vật lý thông qua cơ chế bắt cầu (bridged) nên không tạo ra card VMnet. VMnet8 mặc định sẽ sử dụng cơ chế NAT. Các VMnet khác khi được thêm vào sẽ là Host-Only.



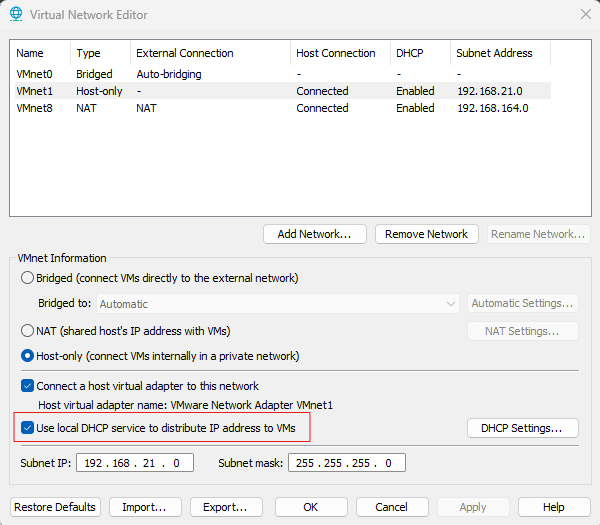
Trong một số trường hợp, có thể card mạng ảo kết nối máy thật với các VMnet chưa được bật lên. Để bật các card này, trên Virtual Network Editor, bạn chọn VMnet cần bật card kết nối từ máy thật vào VMnet, chọn check vào ô Connect a host virtual adapter to this network.

**b.** Card mạng ảo trên máy ảo

Khi bạn tạo một máy ảo mới, card mạng được tạo ra cho máy ảo, những card mạng này hiển thị trên hệ điều hành máy ảo với tên thiết bị như là AMD PCNET PCI hay Intel Pro/1000 MT Server Adapter. Từ VMware Workstation 6.0 trở về sau này máy ảo có thể hổ trợ đến 10 card, các phiên bản trước bị giới hạn ở 3 card mạng. Thêm bớt card mạng bạn nhấn vào nút Add… hoặc Remove… trong Virtual Machine Setting

**c.** DHCP server ảo của Vmnet

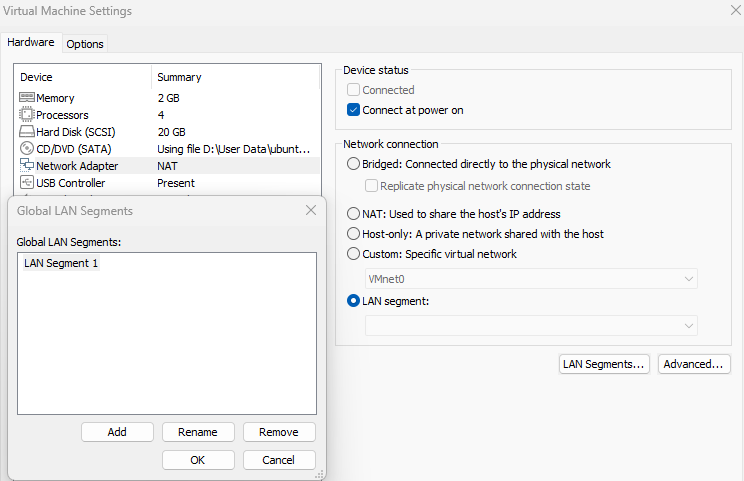
DHCP (Dynamic Host Configuration) server ảo đảm nhiệm việc cung cấp địa chỉ IP cho các máy ảo trong việc kết nối máy ảo vào các Switch ảo không có tính năng Bridged (VMnet0). DHCP server ảo cấp phát địa chỉ IP cho các máy ảo có kết nối với VMnet Host-only và NAT.



Nếu không muốn sử dụng DHCP server ảo của VMnet, bạn chỉ cần bỏ dấu check tại Use local DHCP service to distribute IP address to VMs. Nếu bạn muốn tùy chỉnh lại DHCP, bạn có thể chọn vào DHCP Setting, ở đây, bạn có thể chỉnh lại các tham số thời gian, tham số Scope IP (lưu ý: bạn chỉ có thể sửa lại vùng địa chỉ host chứ không được chỉnh lại vùng network).

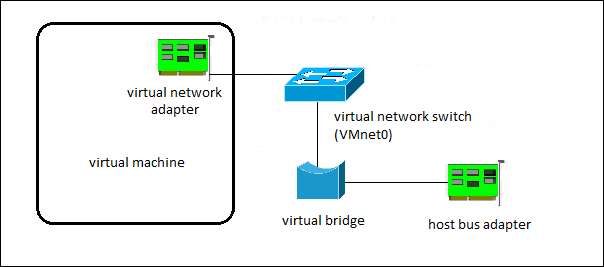
**d**. LAN Segment

Các card mạng của máy ảo có thể gắn kết với nhau thành từng LAN Segment. Không giống như VMnet, LAN Segment chỉ kết nối các máy ảo được gán trong một LAN Segment lại với nhau mà không có những tính năng như DHCP và LAN Segment không thể kết nối ra máy thật như các Virtual Switch VMnet.

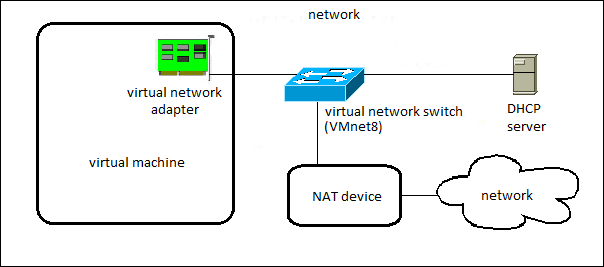


**e.** Các cơ chế hoạt động và các mô hình cơ bản khi cấu hình với switch ảo (VMnet)

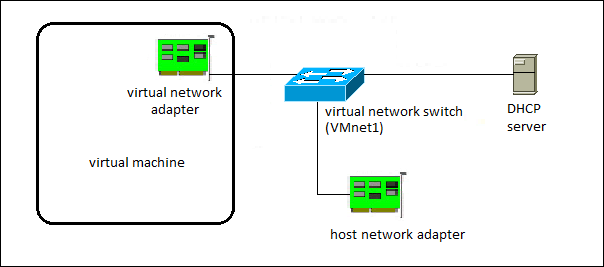
− Chế độ Bridge: Ở chế độ này, card mạng trên máy ảo được gắn vào VMnet0, VMnet0 này liên kết trực tiếp với card mạng vật lý trên máy thật, máy ảo lúc này sẽ kết nối internet thông qua card mạng vật lý và có chung lớp mạng với card mạng vật lý.



− Chế độ NAT: Ở chế độ này, card mạng của máy ảo kết nối với VMnet8, VNnet8 cho phép máy ảo đi ra mạng vật lý bên ngoài internet thông qua cơ chế NAT (NAT device). Lúc này lớp mạng bên trong máy ảo khác hoàn toàn với lớp mạng của card vật lý bên ngoài, hai mạng hoàn toàn tách biệt. IP của card mạng máy ảo sẽ được cấp bởi DHCP của VMnet8, trong trường hợp bạn muốn thiết lập IP tĩnh cho card mạng máy ảo bạn phải đảm bảo chung lớp mạng với VNnet8 thì máy ảo mới có thể đi internet.



− Cơ chế Host-only: Máy ảo được kết nối với VMnet có tính năng Host-only, trong trường hợp này là VMnet1. VMnet Host-only kết nối với một card mạng ảo tương ứng ngoài máy thật (như đã nói ở phần trên). Ở chế độ này, các máy ảo không có kết nối vào mạng vật lý bên ngoài hay internet thông qua máy thật, có nghĩa là mạng VMnet Host-only và mạng vật lý hoàn toàn tách biệt. IP của máy ảo được cấp bởi DHCP của VMnet tương ứng. Trong nhiều trường hợp đặc biệt cần cấu hình riêng, ta có thể tắt DHCP trên VMnet và cấu hình IP bằng tay cho máy ảo.



**1.2.2**. Tìm hiểu về Pfsense

**a.** Giới thiệu

Để bảo vệ hệ thống mạng thì ta có nhiều giải pháp như sử dụng router cisco, dùng firewall cứng, firewall mềm của microsoft như ISA … Những thiết bị như trên rất tốn kinh phí vì vậy đối với các doanh nghiệp vừa và nhỏ thì giải pháp firewall mềm mã nguồn mở là một phương án hiệu quả. Pfsense là một ứng dụng có chức năng định tuyến vào tường lửa mạng và miễn phí dựa trên nền tảng FreeBSD có chức năng định tuyến và tường lửa rất mạnh. Pfsense được cấu hình qua giao diện GUI trên nền web nên có thể quản lý một cách dễ dàng. Nó hỗ trợ lọc theo địa chỉ nguồn, đích, cũng như port nguồn hay port đích đồng thời hỗ trợ định tuyến và có thể hoạt động trong chế độ bridge hay transparent. Nếu sử dụng pfsense là gateway, ta cũng có thể thấy rõ việc hỗ trợ NAT và port forward trên pfsense cũng như thực hiện cân bằng tải hay failover trên các đường mạng.

**b**. Các tính năng trong pfsense

🟊 Aliases

Trong pfsense, firewall không thể có 1 rule gồm nhiều nhóm IP hoặc 1 nhóm port. Vì vậy, điều ta cần làm là gom nhóm các IP, Port hoặc URL vào thành 1 alias . Một alias sẽ cho phép thay thế 1 host, 1 dải mạng, nhiều IP riêng biệt hay 1 nhóm port, URL … Alias giúp ta tiết kiệm được phần lớn thời gian nếu bạn sử dụng một cách chính xác như thay vì sử dụng hàng loạt rule để thiết lập cho nhiều địa chỉ, ta có thể sử dụng 1 rule duy nhất để gom nhóm lại.

🟊 NAT

Pfsense có hỗ trợ nat static dưới dạng nat 1:1. Điều kiện để thực hiện được nat 1:1 là ta phải có IP public. Khi thực hiện nat 1:1 thì IP private được nat sẽ luôn ra ngoài bằng IP public tương ứng và các port cũng tương ứng trên IP public.

Pfsense hỗ trợ nat outbound mặc định với Automatic outbound NAT rule generation. Để cấu hình thủ công, ta chọn Manual Outbound NAT rule generation (AON - Advanced Outbound NAT) và xóa các rule mặc định của pfsense đi đồng thời cấu hình thêm các rule outbound.

Ngoài 3 kiểu Nat: port forward, 1:1 và outbound, pfsense còn hỗ trợ NAT Npt. Phương thức này thực hiện NAT đối với Ipv6.

🟊 Firewall Rules

Là nơi lưu trữ tất cả các luật ra, vào trên pfsense. Mặc định PfSense cho phép mọi kết nối ra, vào (tại cổng LAN có sẵn rule any à any). Ta phải tạo các rule để quản lý mạng bên trong.

🟊 Traffic shaper

Đây là tính năng giúp quản trị mạng có thể tinh chỉnh, tối ưu hóa đường truyền trong pfsense. Trong pfsense, 1 đường truyền băng thông sẽ chia ra các hàng khác nhau. Có 7 loại hàng trong pfsense:

− Hàng qACK: dành cho các gói ACK (gói xác nhận) trong giao thức TCP ở những ứng dụng chính cần được hỗ trợ như HTTP, SMTP … luồng thông tin ACK tương đối nhỏ nhưng lại rất cần thiết để duy trì tốc độ lưu thông lớn.

− Hàng qVoIP: dành cho những loại lưu thông cần đảm bảo độ trễ nghiêm ngặt, thường dưới 10ms như VoIP, video conferences.

− Hàng qGames: dành cho những loại lưu thông cần đảm bảo độ trễ rất chặt chẽ, thường dưới 50ms như SSH, game online …

− Hàng qOthersHigh: dành cho các loại ứng dụng quan trọng có tính tương tác rất cao, cần đáp ứng nhanh, cần độ trễ thấp như: NTP, DNS, SNMP …

− Hàng qOthersDefault: dành cho các giao thức ứng dụng quan trọng có tính tương tác vừa, cần độ đáp ứng nhất định như HTTP, IMAP …

− Hàng qOthersLow: dành cho các giao thức ứng dụng quan trọng nhưng có tính tương tác thấp như SMTP, POP3, FTP

− Hàng qP2P: dành cho cho các ứng dụng không tương tác, không cần đáp ứng nhanh như bittorrent

Mặc định trong pfsense, các hàng sẽ có độ ưu tiên từ thấp đến cao: qP2P < qOthersLow < qOthersDefault < qOthersHigh < qGames < qACK < qVoIP.

Ta có thể chỉnh lại độ ưu tiên priority cũng như dung lượng băng thông bandwidth mặc định mà các hàng chiếm để nâng cao băng thông cho các hàng tương ứng.

Pfsense cũng hỗ trợ giới hạn tốc độ download/upload của 1 IP hoặc 1 dải IP với ta thiết lập thông số tại phần limiter. Firewall pfsense hỗ trợ chặn những ứng dụng chạy trên layer 7 – application trong mô hình OSI như sip, ftp, http … trong phần Layer 7.

🟊 VPN

Một tính năng khác không thể thiếu đối với các gateway là VPN. Pfsense cũng hỗ trợ VPN qua 4 giao thức: IPSec, L2TP, PPTP và OpenVPN.

🟊 Monitor băng thông

Pfsense có rất nhiều plugin hỗ trợ monitor băng thông. Sau đây là 1 số plugin thông dụng:

RRD Graphs

Đây là tool mặc định có sẵn khi cài pfsense. Với RRD graphs, ta có thể theo dõi được trạng thái của server: memory, process … hay với băng thông của các đường truyền LAN, WAN … Một nhược điểm của RRD Graphs là không theo dõi được dung lượng từng IP.

Lightsquid

Lightsquid là package hỗ trợ xem report trên pfsense sau khi đã cài gói squid. Với Lightsquid, ta có thể check dung lượng mỗi IP sử dụng theo ngày. Tổng dung lượng ngày hôm đó sử dụng hay các trang web đã vào …

BandwidthD

1 plugin nữa có thể monitor dung lượng sử dụng của IP là BandwidthD.BandwidthD thống kê dữ liệu theo từng IP, dung lượng gửi, nhận, các giao thức sử dụng như FTP, HTTP …

Ntop

1 plugin thường được sử dụng nữa là Ntop. Với Ntop, ta có thể theo dõi băng thông hiện tại IP nào sử dụng lớn nhất, dung lượng tải của cổng, kết nối tới internet …

**c**. Tổng kết

Hoàn toàn miễn phí, giá cả là ưu thế vượt trội của tường lửa pfsense. Tuy nhiên, rẻ không có nghĩa là kém chất lượng, tường lửa pfsense hoạt động rất ổn định với hiệu năng cao, tối ưu hóa mã nguồn và hệ điều hành.

Vì vậy pfsense không cần phần cứng phải mạnh. Pfsense hoạt động như một thiết bị mạng tổng hợp với đây đủ tính năng và sẵn sàng bất cứ lúc nào. Pfsense hỗ trợ rất nhiều plugin để thiết lập thêm các tính năng hữu ích mà người dùng thấy cần thiết.

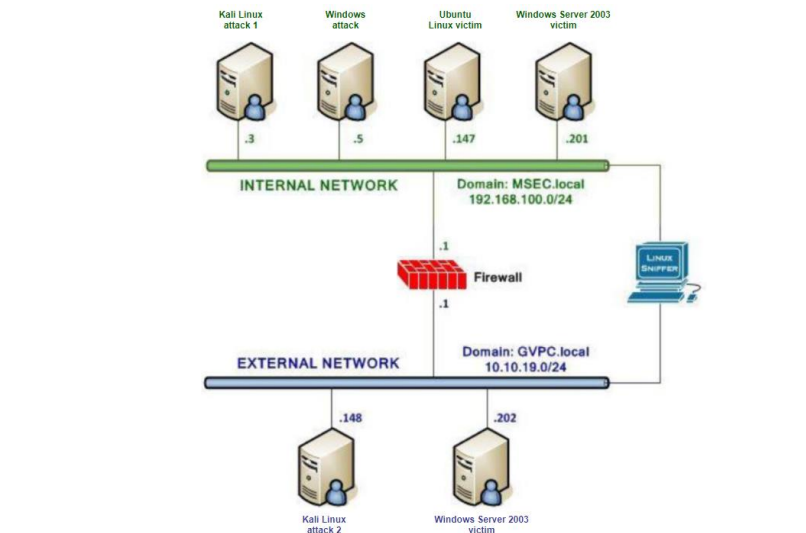
Như vậy, tường lửa pfSense là sự kết hợp hoàn hảo và mạnh mẽ, đem lại sự hợp lý cho các nhà tài chính, và sự tin tưởng cho các nhà quản trị.

1. NỘI DUNG THỰC HÀNH
   1. Chuẩn bị môi trường

* Phần mềm ảo hóa, chẳng hạn: VMWare Workstation.
* Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows và Linux.
* File cài đặt tường lửa Pfsense
  1. Các bước thực hiện

**2.2.1** Cấu hình topo mạng

Cài đặt và cấu hình hệ thống theo topo mạng và thông tin như mô tả dưới đây (bao gồm cài đặt các máy ảo)



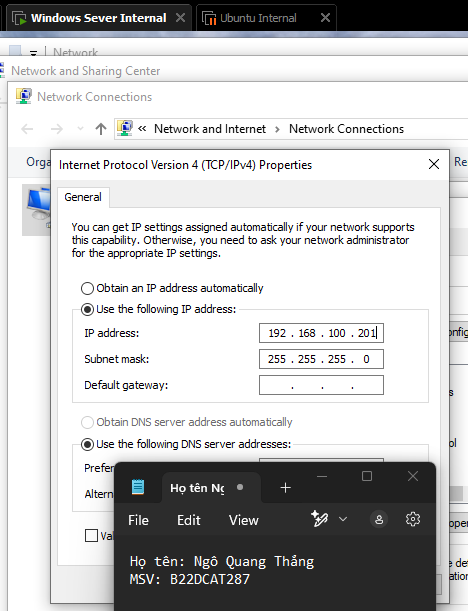
|  |  |
| --- | --- |
| Máy Kali Linux attack 1 trong mạng Internal | IP: 192.168.100.3  Mật khẩu root: password |
| Máy Windows Server 2019 Victim trong mạng Internal | IP: 192.168.100.201  Mật khẩu root: password |
| Máy Linux Victim trong mạng Internal | IP: 192.168.100.147  Mật khẩu root: password |
| Máy pfSense Firewall | IP: 10.10.19.1, 192.168.100.1  Mật khẩu: admin/pfsense |
| Máy Linux Attack trong mạng External | IP: 10.10.19.148  Mật khẩu root: password |
| Máy Windows Server 2019 Victim trong mạng External | IP: 10.10.19.202  Mật khẩu root: password |

Điều chỉnh địa chỉ Ip cho dải máy Internal:

Với máy Windows Sever 2019: *Network -> Network and Sharing Center -> Network Connections -> Internet protocol Version4*

Điều chỉnh Ip address: *192.168.100.201*

Sunet mask: *255.255.255.0*



Với máy kali attack1:

*sudo nano /etc/network/interfaces*

Thay đổi ip tĩnh:

*auto eth0*

*iface eth0 inet static*

*address 192.168.100.3*

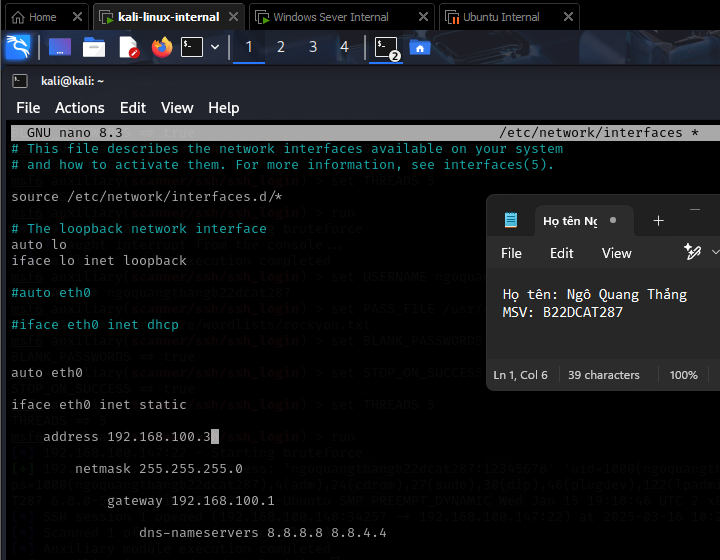
*netmask 255.255.255.0*

*gateway 192.168.100.1*

*dns-nameservers 8.8.8.8 8.8.4.4*

Sau khi thay đổi thực hiện khởi động lại:

*sudo systemctl restart networking*



Với máy ubuntu internal:

*sudo gedit /etc/netplan/01-network-manager.yaml*

Thay đổi ip tĩnh:

*network:*

*version: 2*

*ethernets:*

*eth0:*

*dhcp4: no*

*addresses:*

*- 192.168.100.147/24*

*gateway4: 192.168.100.1*

*nameservers:*

*addresses:*

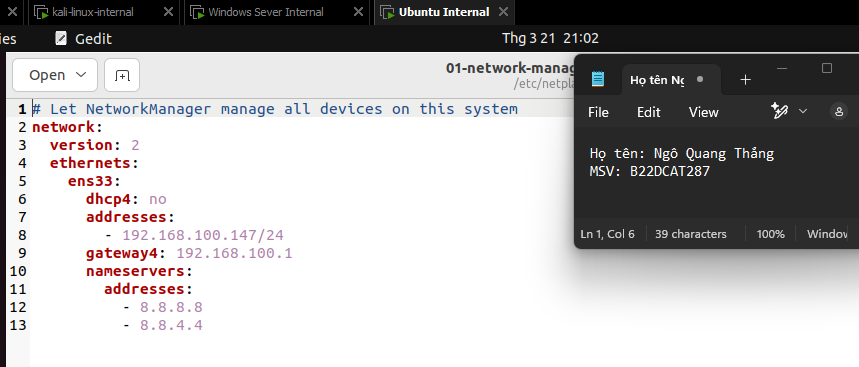
*- 8.8.8.8*

*- 8.8.4.4*

Sau đó thực hiện lưu lại thay đổi trong tệp

Lưu và áp dụng cấu hình:

*sudo netplan apply*

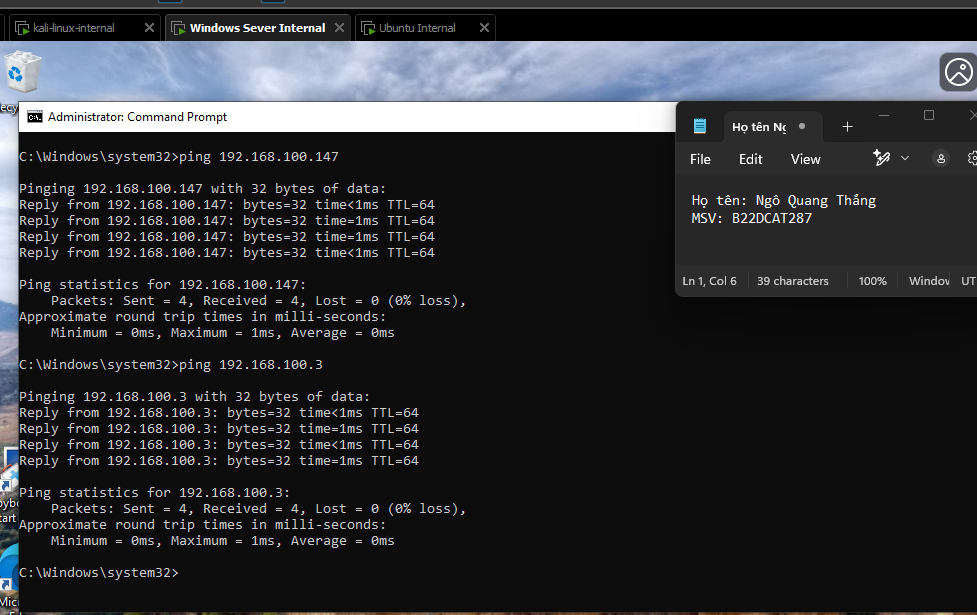


Thực hiện kiểm tra các máy có thể ping tới nhau chưa:

Từ máy Windows Sever Internal:

*ping 192.168.100.147*

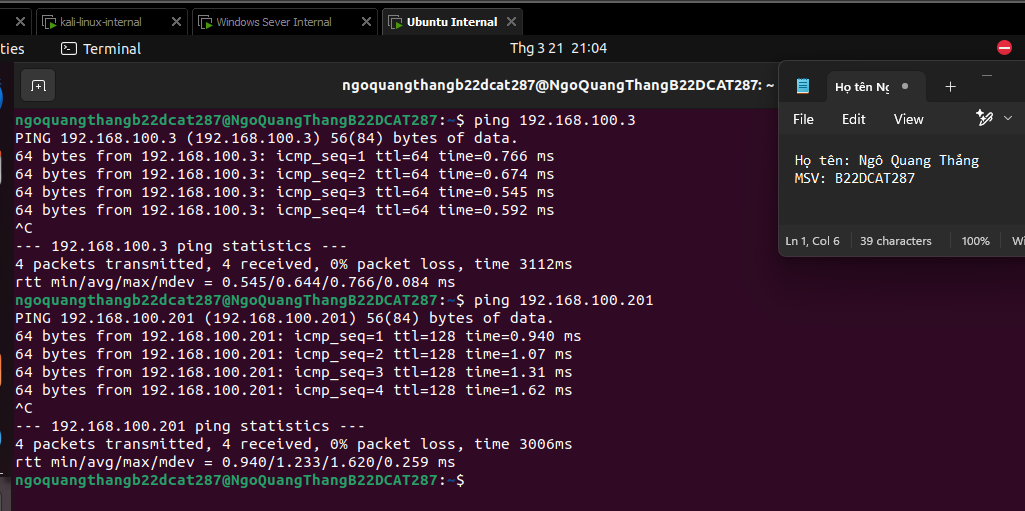
*ping 192.168.100.3*



Từ máy ubuntu internal:

*ping 192.168.100.3*

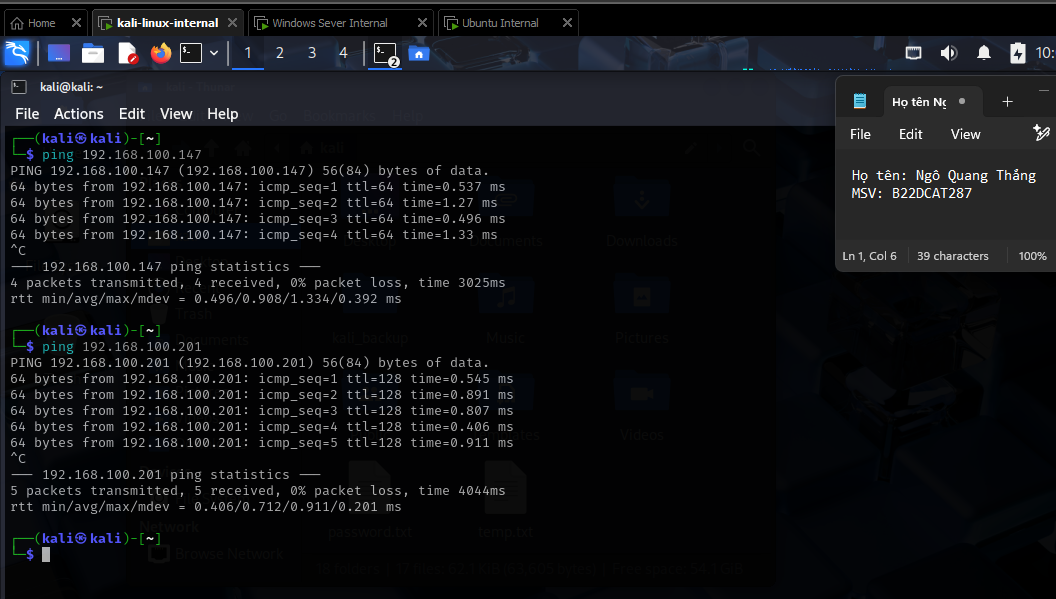
*ping 192.168.100.201*



Từ máy kali attack 1:

*ping 192.168.100.147*

*ping 192.168.100.201*

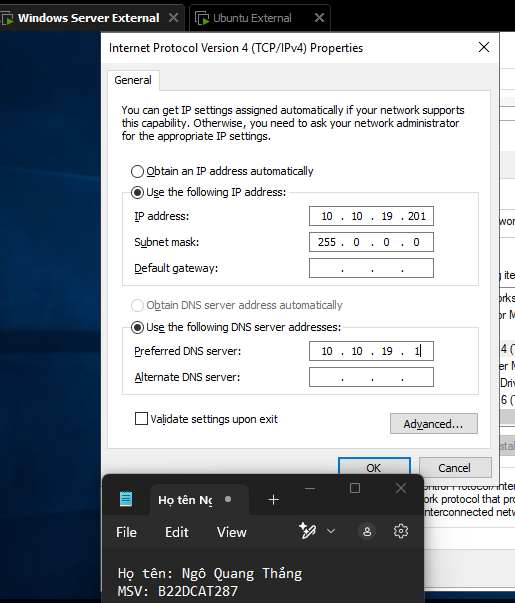


Điều chỉnh ip cho dải mạng external:

Với máy Windows Sever tương tự với máy bên internal:

Điều chỉnh Ip address: *192.168.100.201*

Sunet mask: *255.255.255.0*



Với máy kali attack 2 cũng tương tự như bên kali attack 1:

*sudo nano /etc/network/interfaces*

Thay đổi ip tĩnh:

*auto eth0*

*iface eth0 inet static*

*address 10.10.19.148*

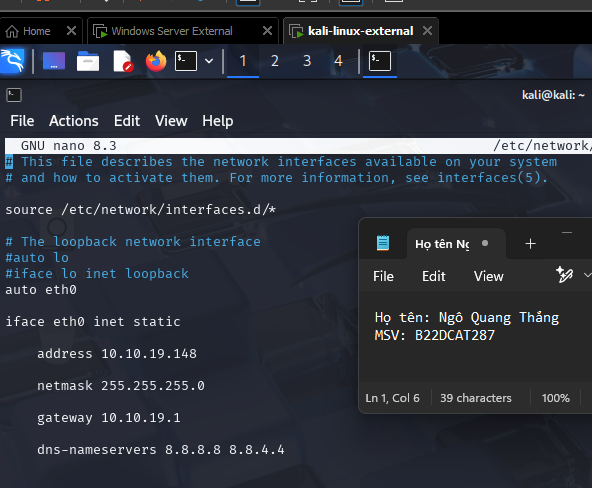
*netmask 255.255.255.0*

*gateway 10.10.19.1*

*dns-nameservers 8.8.8.8 8.8.4.4*

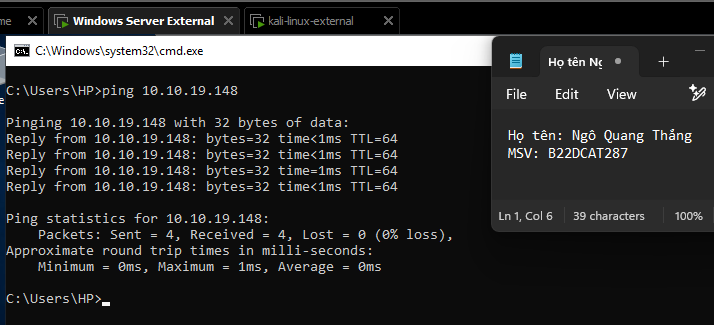
Sau khi thay đổi thực hiện khởi động lại:

*sudo systemctl restart networking*

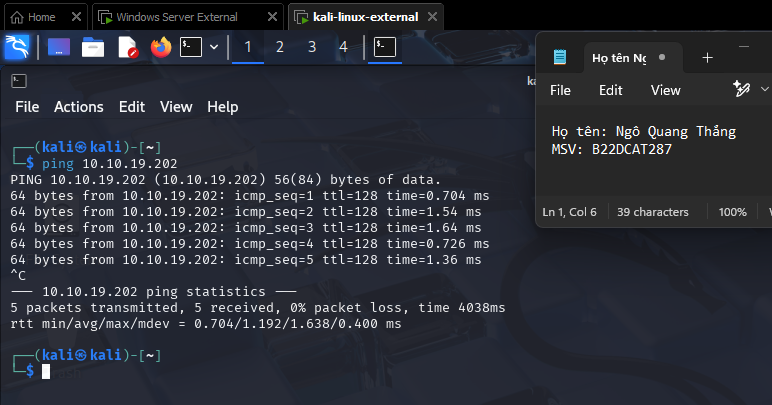


Kiểm tra 2 máy đã có thể ping tới nhau chưa:

Windows Sever External: *ping 10.10.19.148*



Kali attack 2: *ping 10.10.19.202*



**2.2.2** Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

Sau khi cài đặt pfsense; thực hiện cấu hình lại địa chỉ ip cho mạng LAN, WAN

Với mạng WAN: Lựa chọn *1*

Configure IPv4 address WAN interface via DHCP: Lựa chọn “*n*” để thực hiện

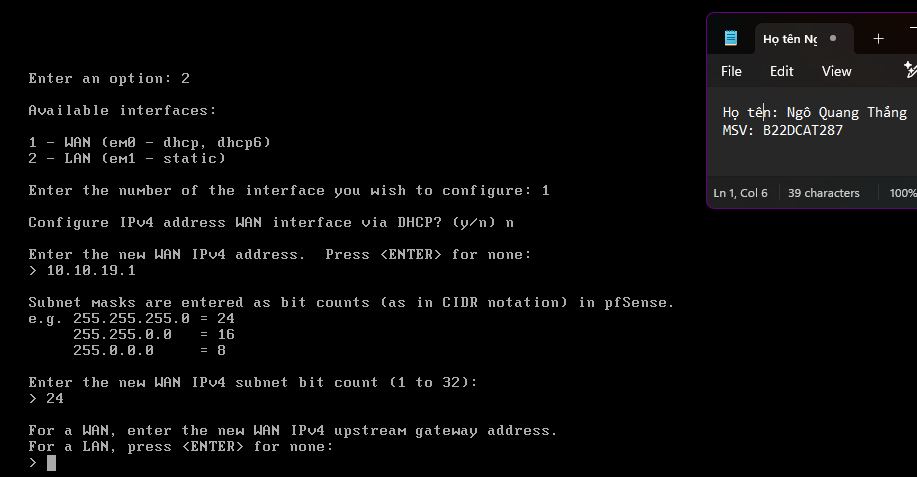
cài địa chỉ Ip thủ công -> *Ip: 10.10.19.1*

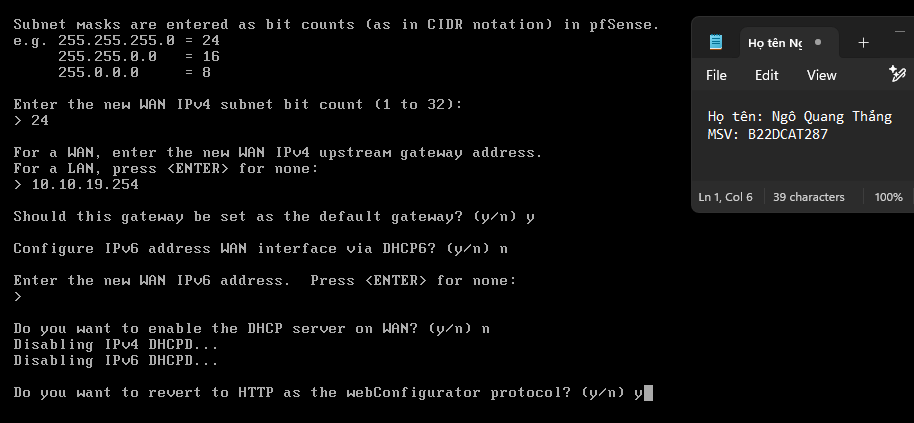
Lựa chọn “*24*” để sử dụng Subnetmask 255.255.255.0

For a LAN có thể bỏ qua hoặc : *10.10.19.254*

Phần Should this gateway be set the default gateway: thực hiện chọn yes

Bỏ qua thực hiện cài Ip v6 -> sau đó restart





Với mạng LAN, thực hiện tương tự như WAN:

Với mạng LAN: Lựa chọn 2

Configure IPv4 address WAN interface via DHCP: Lựa chọn “*n*” để thực hiện

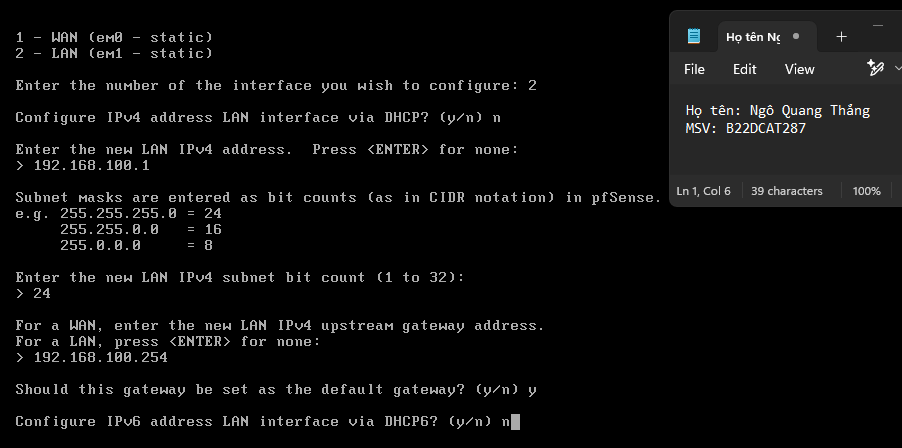
cài địa chỉ Ip thủ công -> Ip: *192.168.100.1*

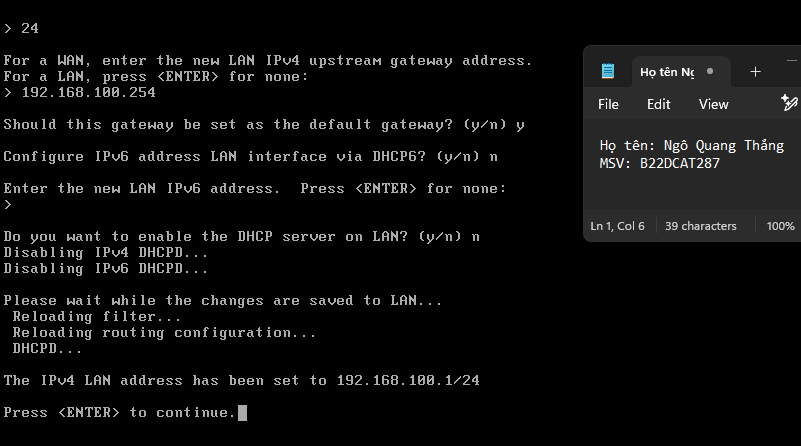
Lựa chọn “*24*” để sử dụng Subnetmask *255.255.255.0*

For a LAN có thể bỏ qua hoặc : *192.168.100.254*

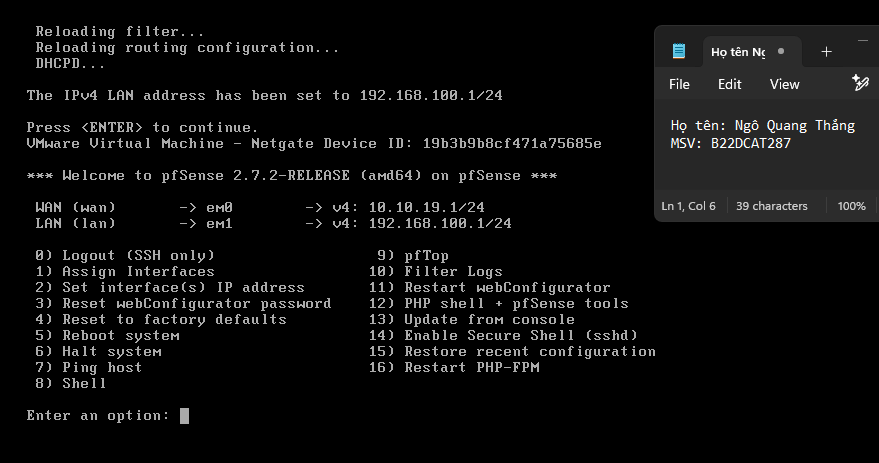
Phần Should this gateway be set the default gateway: thực hiện chọn yes

Bỏ qua thực hiện cài Ip v6 -> sau đó restart





Kết quả sau khi cài đặt lại địa chỉ Ip:

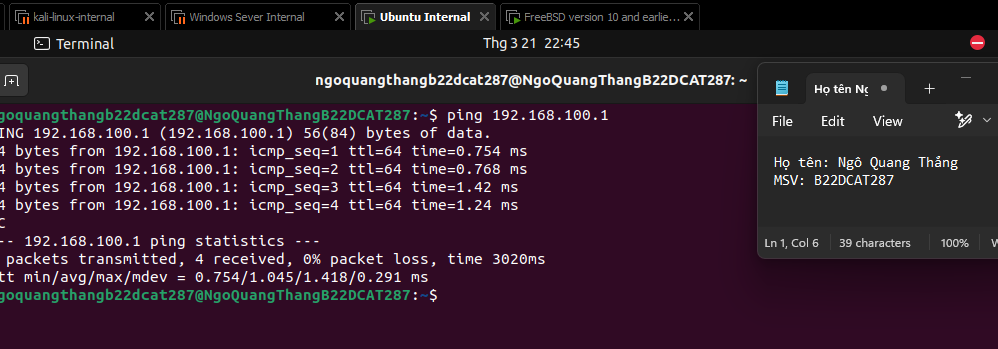


1. Cấu hình ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal.

Các bước lần lượt như sau:

o Trên máy Linux victim(Ubuntu Intenal) thực hiện kiểm tra kết nối đến pfsense bằng cách ping đến:

*ping 192.168.100.1*

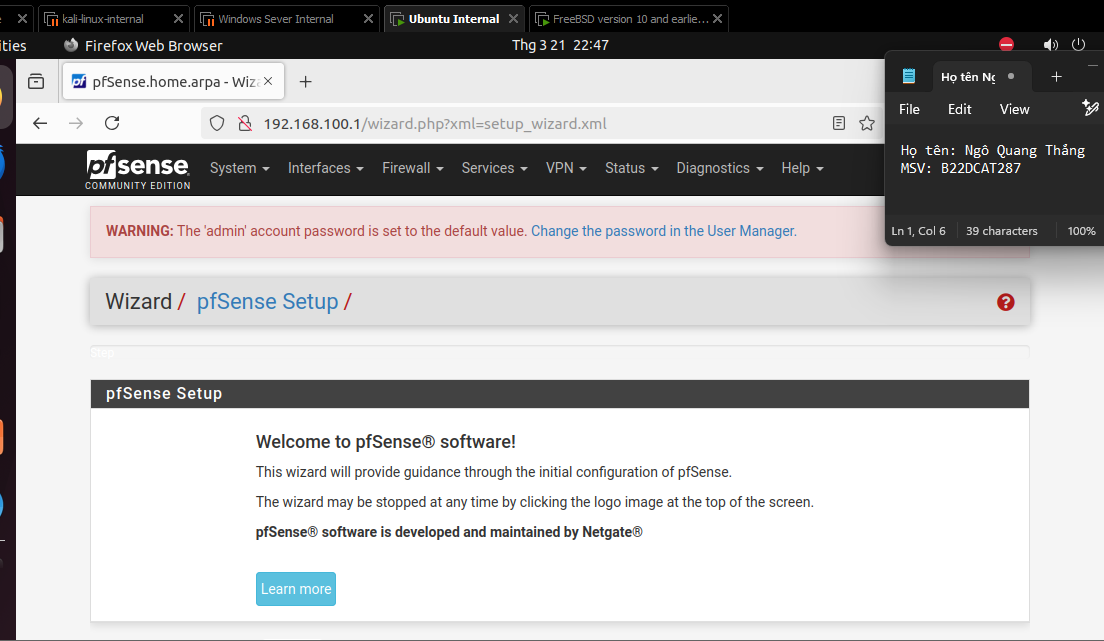


o Trên máy Linux victim(Ubuntu Internal) ở mạng trong, vào <http://192.168.100.1> để cấu hình pfsense qua giao diện web.(Frefox Browser)

Đăng nhập với:

Username: *admin*

Password: *pfsense*

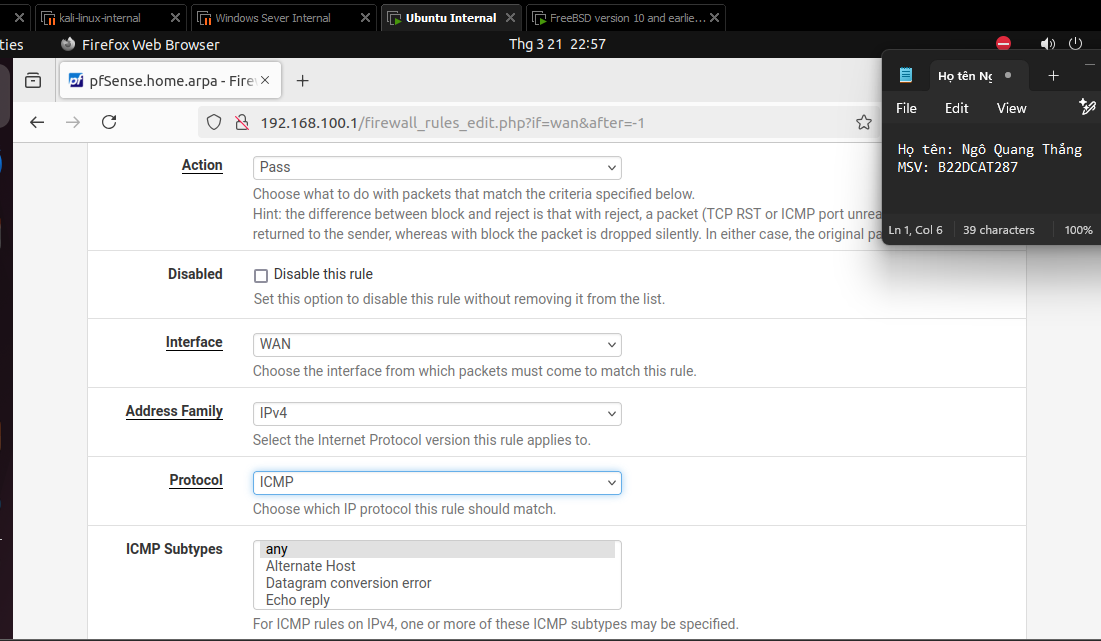


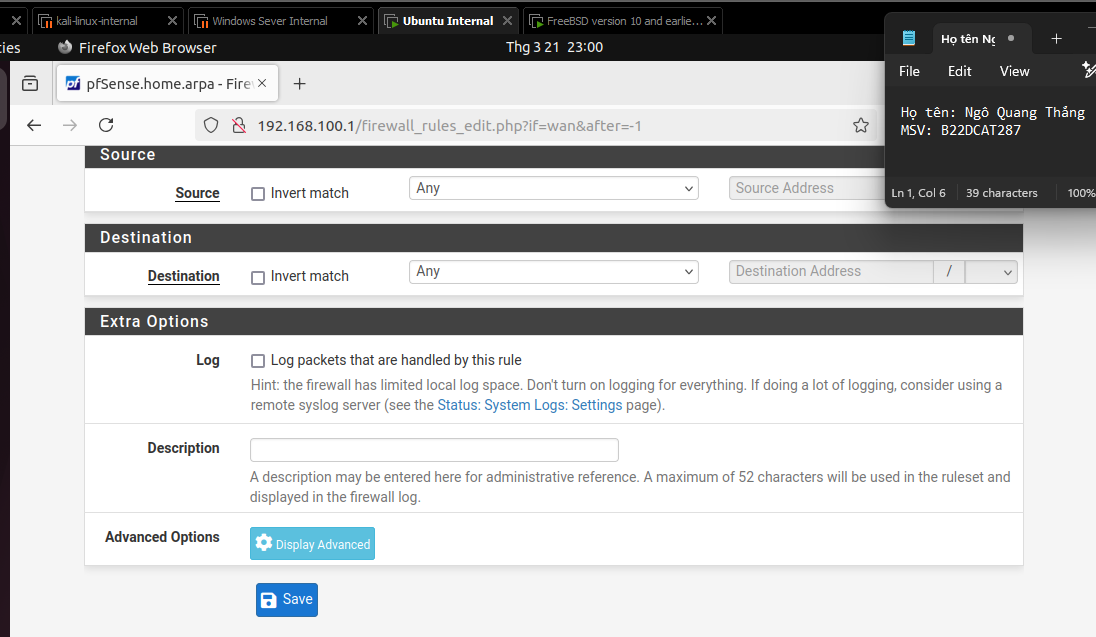
o Cấu hình luật firewall để cho phép luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1

Lựa chọn *Firewall ->Rules -> Add* để điều chỉnh:

Thay đổi Protocol: *ICMP*

ICMP Subtypes: *any*



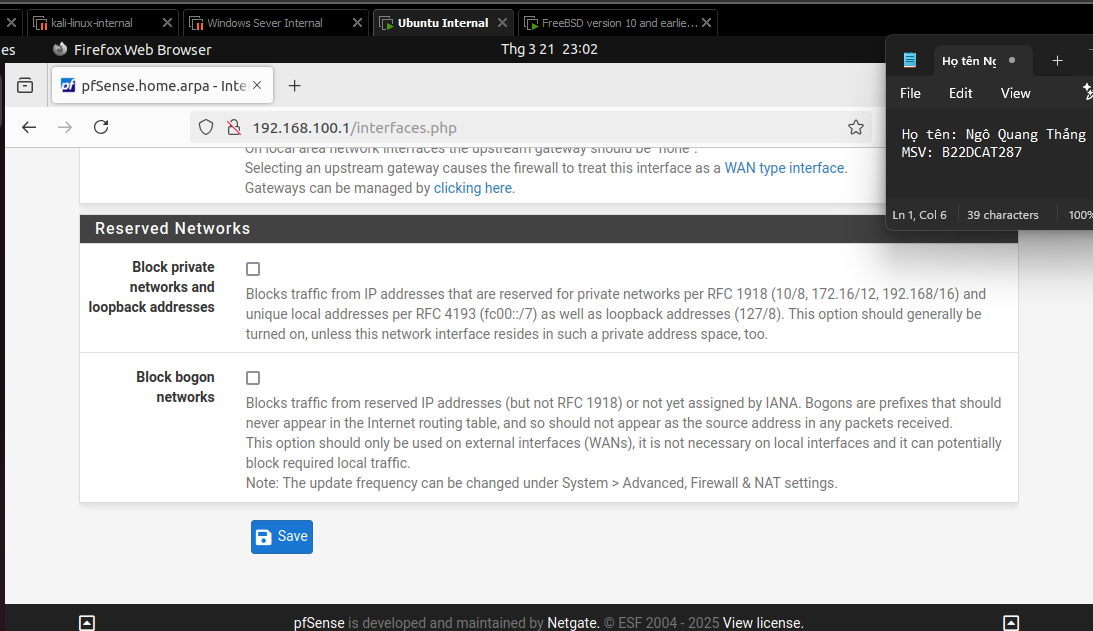


o Sau khi lưu lại thay đổi:

Thực hiện tắt chặn của firewall:

Block private network and loopack address

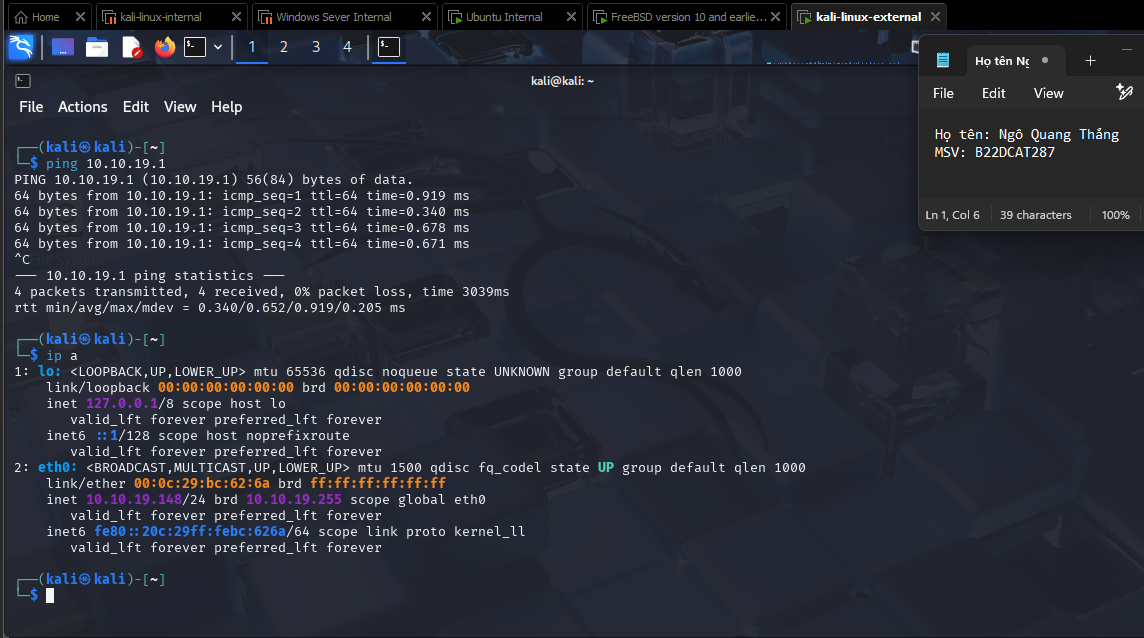
Block bogon networks





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

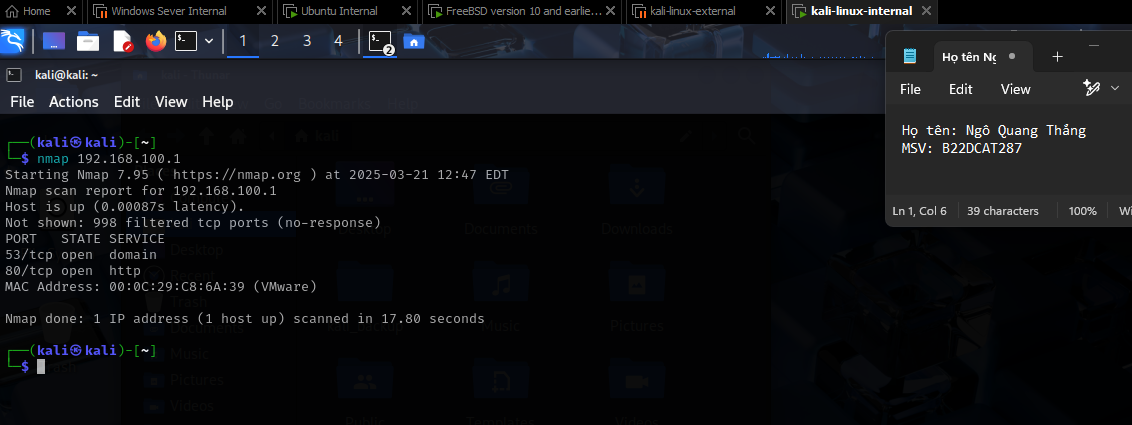
*ping 10.10.19.1* -> thành công



o Trả lời câu hỏi:

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

o Theo mặc định, có 2 cổng TCP mở trên giao điện mạng Internal của Pfsense. Xem và kiểm tra: nmap 192.168.100.1



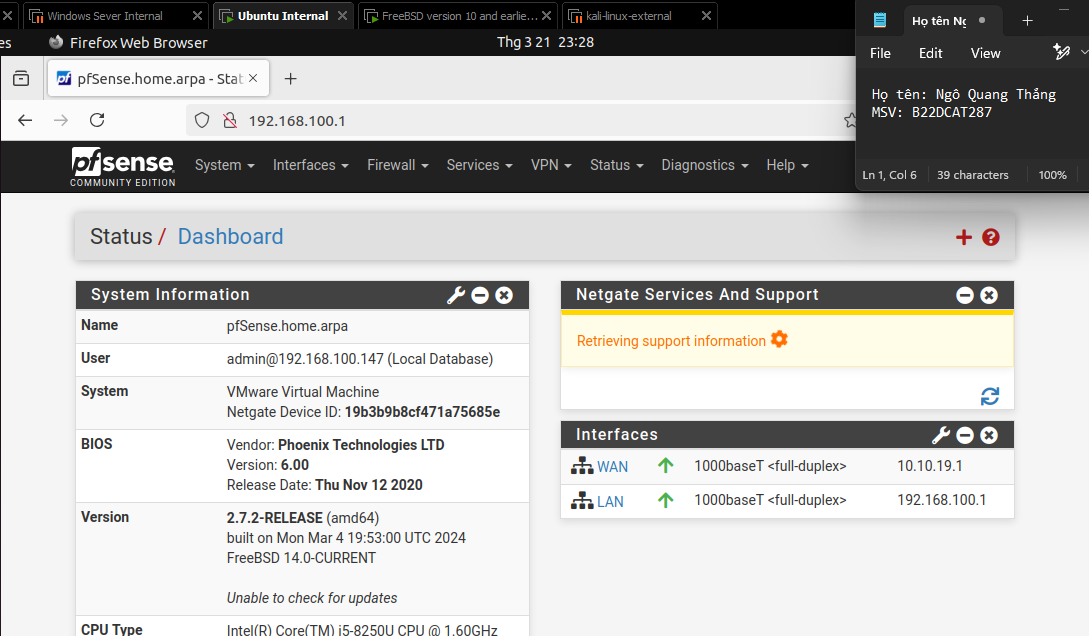
− Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng ngoài của pfSense?

o Theo mặc định, không có cổng TCP nào mở trên giao điện mạng External của Pfsense. Xem và kiểm tra: nmap 10.10.19.1

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

a) Cấu hình tường lửa cho phép 1 cổng và chuyển hướng lưu lượng:

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



o 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.

Thực hiện lựa chọn: *Firewall -> NAT*

Lựa chọn Add để điều chỉnh

Ví trí Protocol: *TCP*

Destination port range lựa chọn: *SSH*(from port – to port)

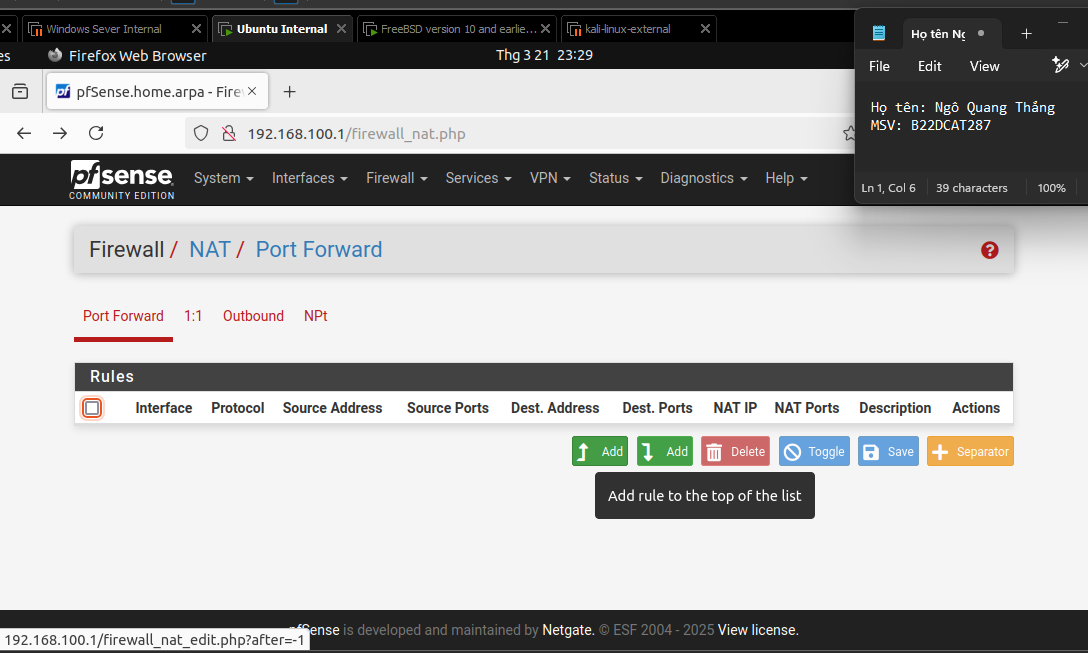
Redirect target IP thay đổi: *192.168.100.147*

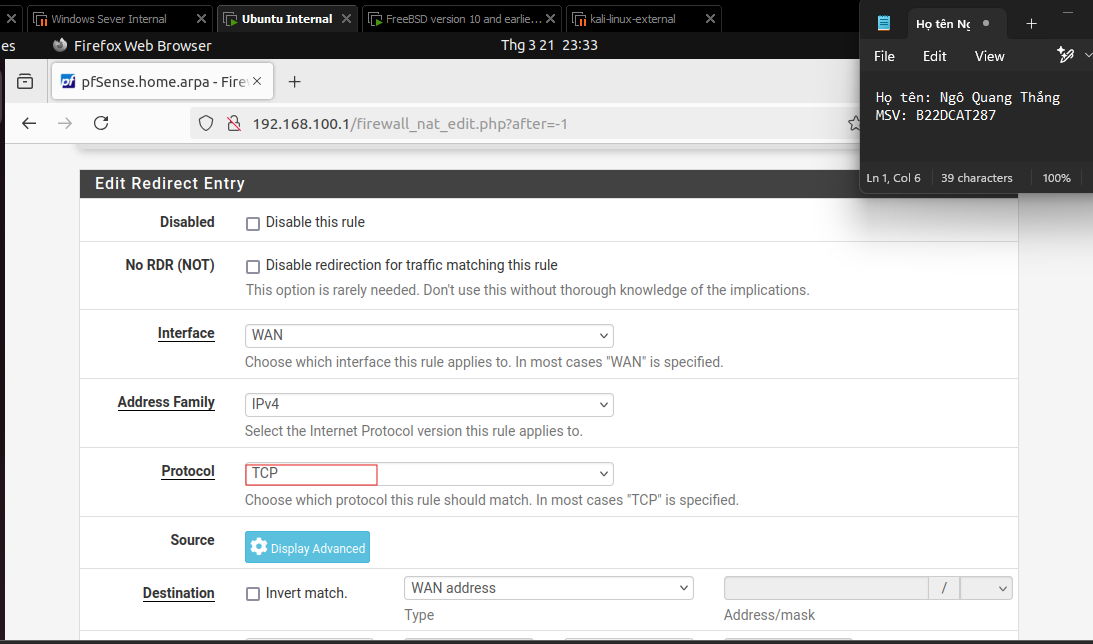
Redirect tager port lựa chọn : *SSH*

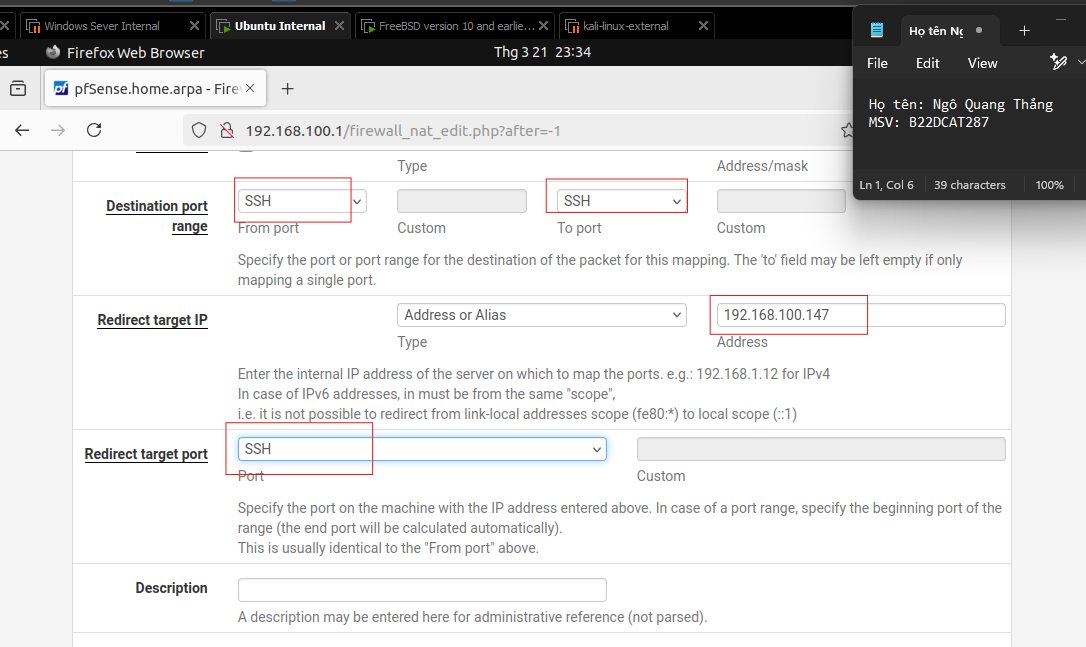
NAT reflection: *use system default*

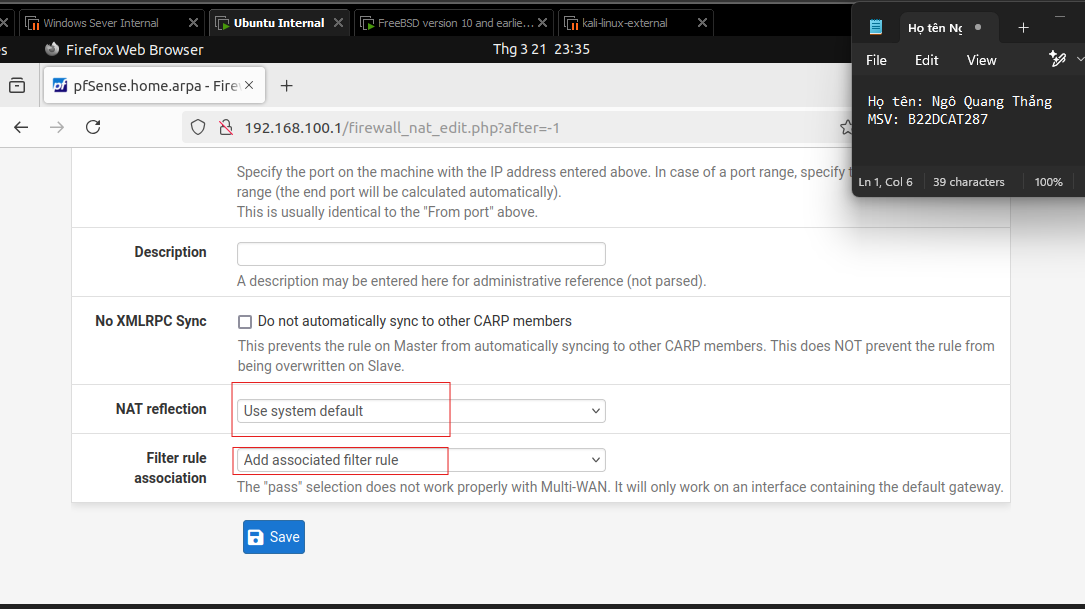
Filter ruler association*: Add associated filter rule*

* Thực hiện lưu thay đổi





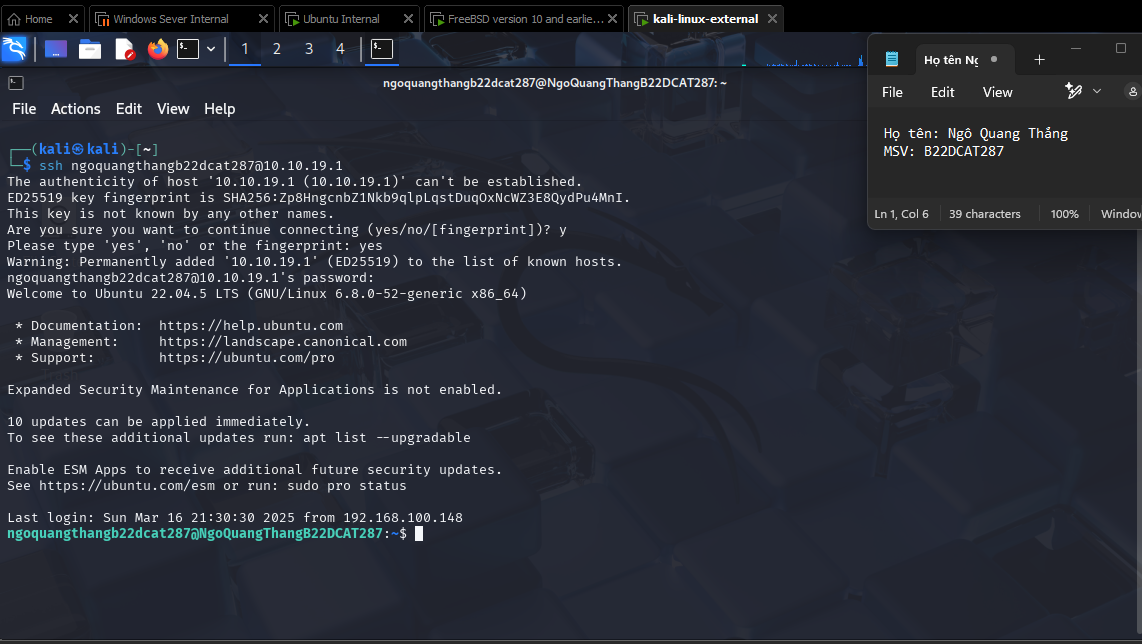


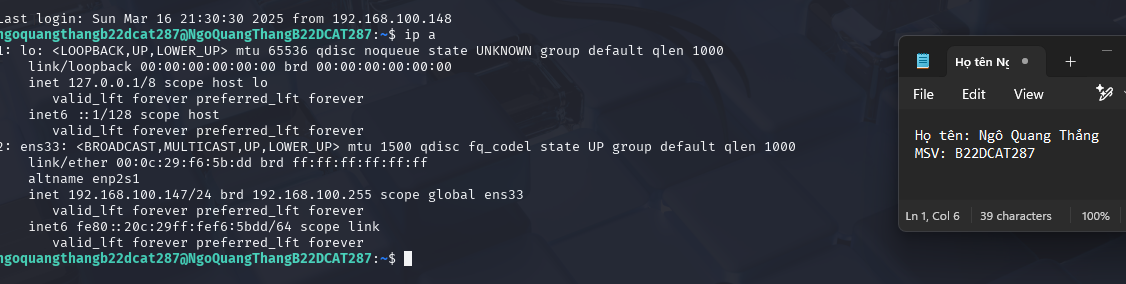


o Kiểm tra bằng cách truy cập ssh tới 10.10.19.1, rồi gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?

*ssh* [*ngoquangthangb22dcat287@10.10.19.1*](mailto:ngoquangthangb22dcat287@10.10.19.1)

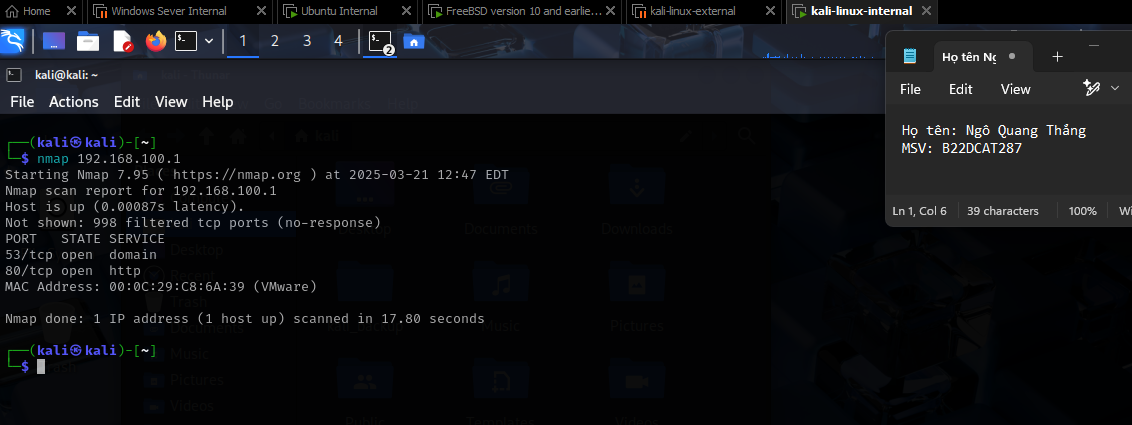
*ip a*





o Kiểm tra các cổng được phép truy cập trên mạng Internal bằng cách gõ lệnh trên máy Kali Linux trong mạng Internal:

*nmap 192.168.100.1* -> Các cổng 53/tcp; 80/tcp



TÀI LIỆU THAM KHẢO

1. Lab 7 pfsense firewall của CSSIA CompTIA Security+®
2. Advanced Penetration Testing for Highly-Secured Environments Second Edition

[3] Giới thiệu về Pfsense:

https://viblo.asia/p/network-gioi-thieu-vepfsense-N0bDM6LXv2X4