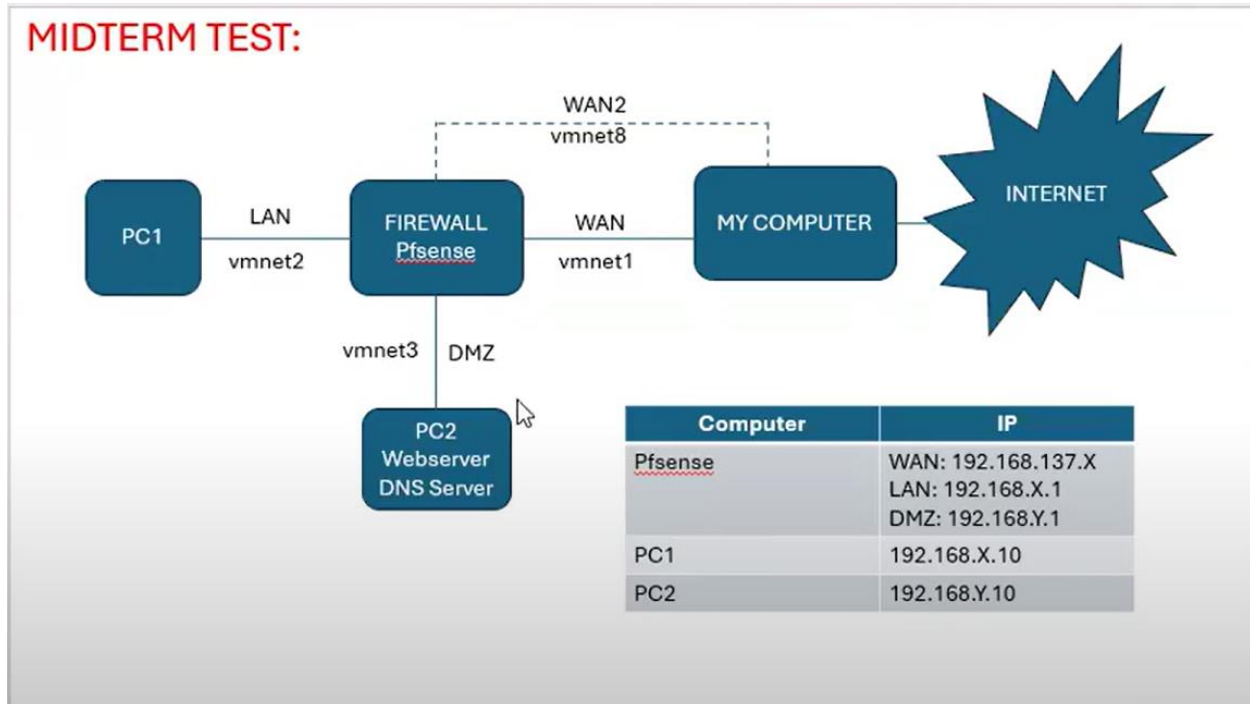


MÔN TRIỂN KHAI AN NINH HỆ THỐNG

Phúc Lâm

GVHD: Đỗ Hà Phương

MIDTERM TEST:

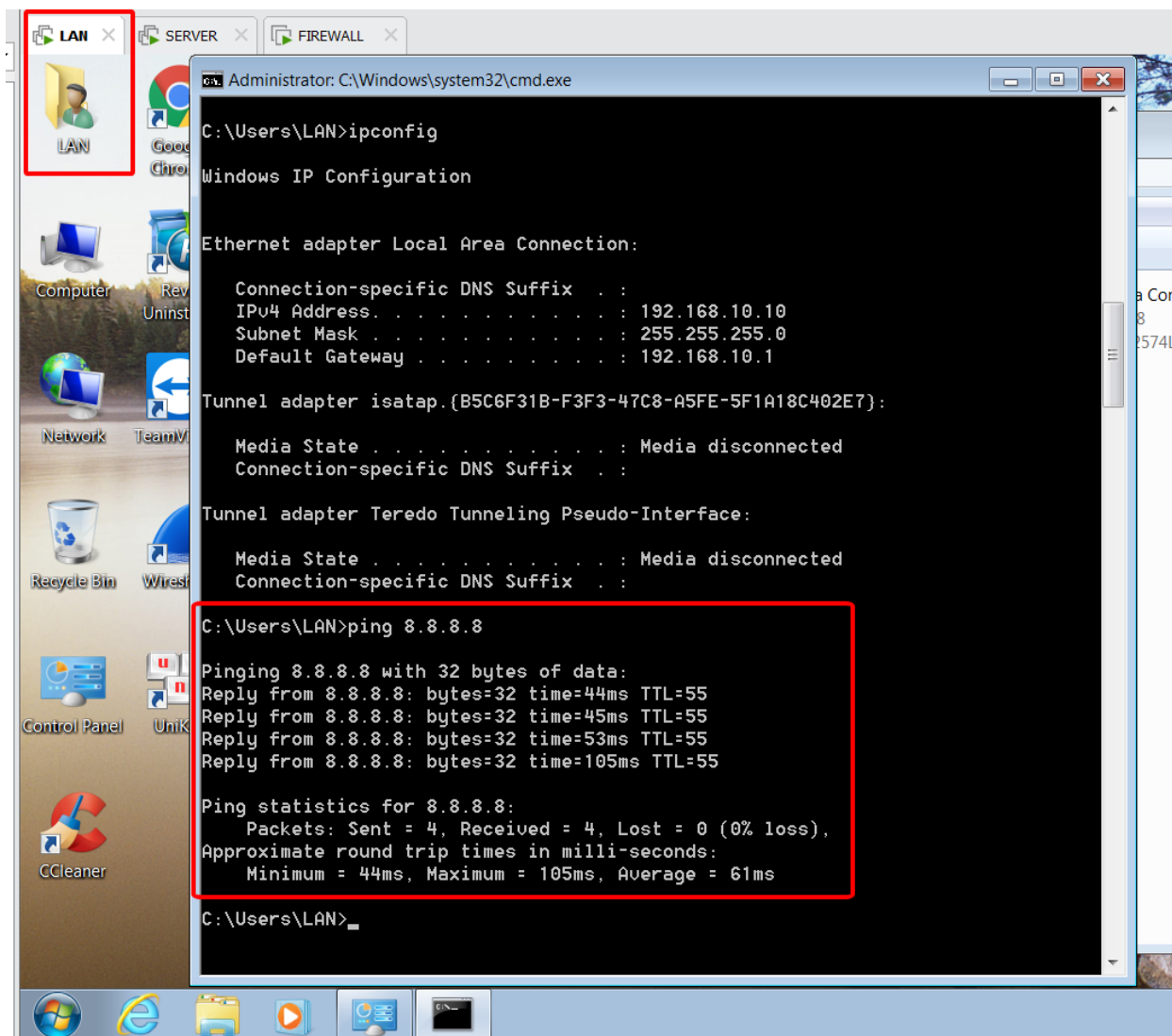


Mission deployments:

1. Cấu hình PfSense, LAN. Kết quả LAN truy cập Internet (1đ)
2. Tạo Alias cấm IP LAN truy cập Internet: 192.168.X.100-192.168.X.200 (1đ)
3. Tạo Alias cấm LAN truy cập: www.tp-link.com, www.shopee.vn, shopee.vn
4. Thiết lập time: Asia/Ho Chi Minh, lập lịch cấm LAN truy cập Internet giờ hành chính
5. Chỉ cho LAN truy cập TCP 80, 443. Kiểm tra LAN chỉ kết nối HTTP bằng IP
6. Mở và chặn DNS tại UDP port 53
7. Mở và chặn ICMP LAN ping ra Internet
8. Thiết lập DNS, WEB Server tại vùng DMZ
9. Public WEB Server
10. Cấu hình MultiGateway WAN1, WAN2 để dự phòng mất kết nối Internet.

SINH VIÊN THỰC HIỆN

1. Cấu hình PfSense, LAN. Kết quả LAN truy cập Internet (1đ)



2. Tạo Alias cấm IP LAN truy cập Internet: 192.168.X.100-192.168.X.200 (1đ)

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect.

IP Ports URLs All

Firewall Aliases IP		Description	Actions
Name	Values		
CamIPLAN100_200	192.168.10.100, 192.168.10.101, 192.168.10.102, 192.168.10.103, 192.168.10.104, 192.168.10.105, 192.168.10.106, 192.168.10.107, 192.168.10.108, 192.168.10.109...		Edit Delete

[Add](#) [Import](#)

Tạo rules

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN OPT1

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	8 / 1.28 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	Settings
<input type="checkbox"/>	0 / 0 B	IPv4 *	CamIPLAN100_200	*	*	*	*	none			Anchor Edit Copy Delete
<input type="checkbox"/>	12 / 11.65 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	Anchor Edit Copy Delete
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.

Đổi IP của LAN sang vùng cấm IP để test kết quả = không truy cập được internet

The screenshot shows the pfSense Firewall Rules configuration interface on the left and a Windows command prompt on the right.

pfSense Firewall Rules Configuration:

The "Rules (Drag to Change Order)" table is displayed with the following data:

	States	Protocol	Source	Port	Destination
<input type="checkbox"/>	8 / 1.28 MiB	*	*	*	LAN Add
<input type="checkbox"/>	0 / 0 B	IPv4 *	CamiPLAN100_200	*	*
<input type="checkbox"/>	12 / 11.65 MiB	IPv4 *	LAN net	*	*
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*

Windows Command Prompt:

```
C:\Users\LAN>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.{B5C6F31B-F3F3-47C8-A5FE-5F1A18C402E7}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\LAN>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\LAN>
```

3. Tạo Alias cấm LAN truy cập: www.tp-link.com, www.shopee.vn, shopee.vn

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Aliases / IP

The alias list has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

IP Ports URLs All

Name	Values	Description	Actions
CamIPLAN100_200	192.168.10.100, 192.168.10.101, 192.168.10.102, 192.168.10.103, 192.168.10.104, 192.168.10.105, 192.168.10.106, 192.168.10.107, 192.168.10.108, 192.168.10.109		Edit Delete
CamLanTruyCap	www.facebook.com, www.tp-link.com, www.shopee.vn		Edit Delete

[Add](#) [Import](#)

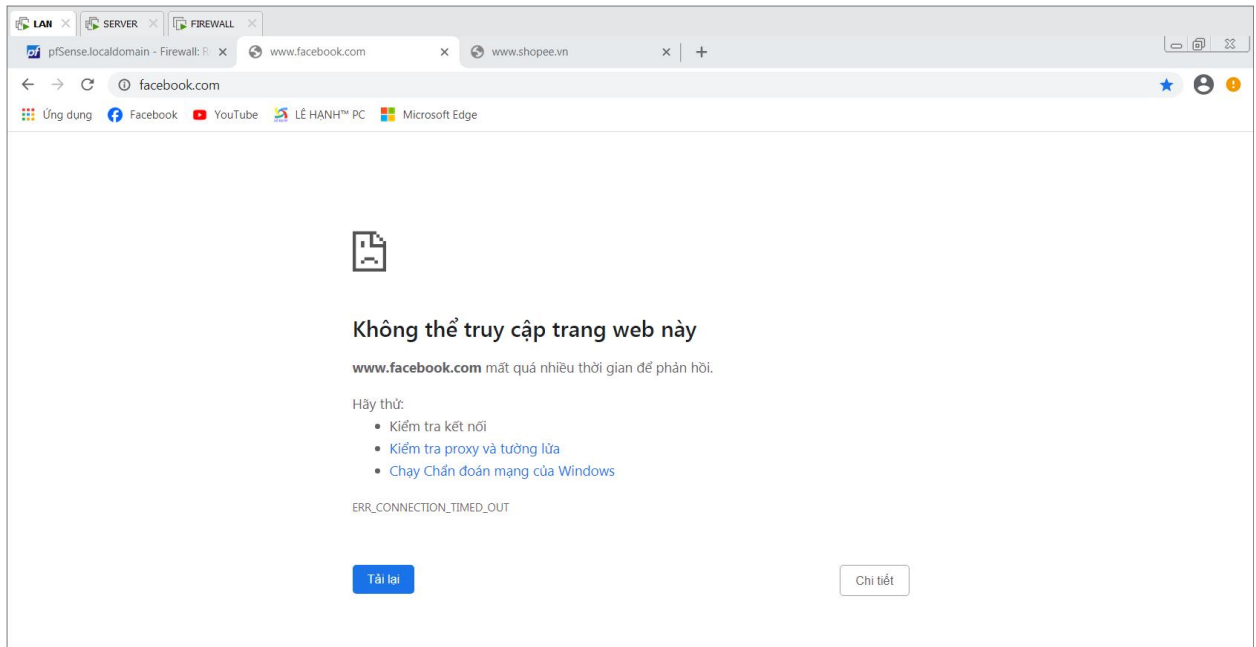
Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

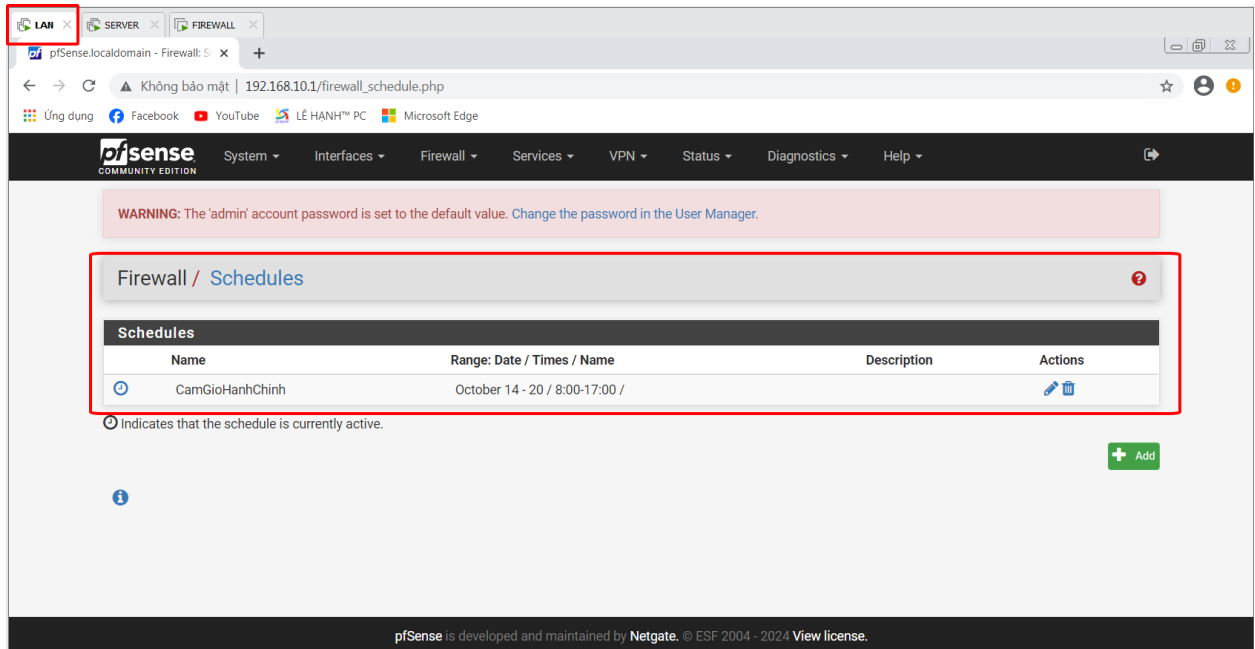
Floating WAN LAN OPT1

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	4 / 1.42 MiB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	Edit
<input type="checkbox"/>	✗	0 / 0 B	IPv4 *	*	CamLanTruyCap	*	*	none			Anchor Edit Copy Delete
<input type="checkbox"/>	✗	0 / 0 B	IPv4 *	*	CamIPLAN100_200	*	*	none			Anchor Edit Copy Delete
<input type="checkbox"/>	✓	25 / 12.33 MiB	IPv4 *	*	LAN net	*	*	none		Default allow LAN to any rule	Anchor Edit Copy Delete
<input type="checkbox"/>	✓	0 / 0 B	IPv6 *	*	LAN net	*	*	none		Default allow LAN IPv6 to any rule	Anchor Edit Copy Delete

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)

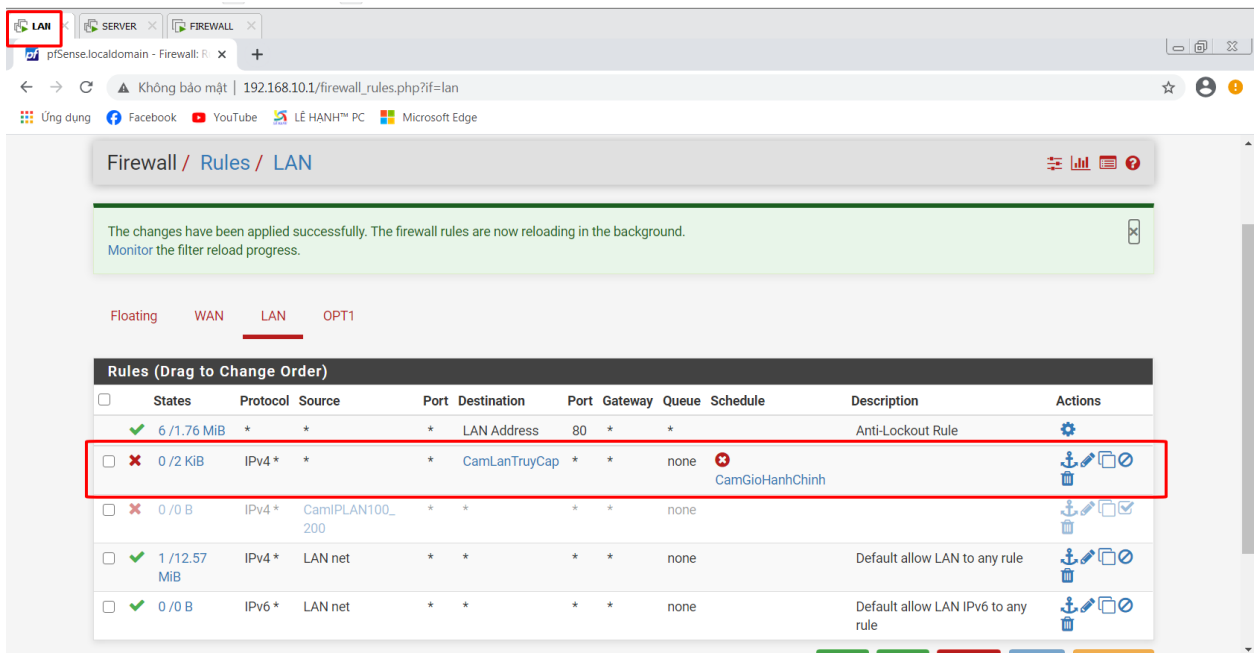


4. Thiết lập time: Asia/Ho Chi Minh, lập lịch cấm LAN truy cập Internet giờ hành chính



The screenshot shows the pfSense web interface. The 'LAN' tab is selected in the top navigation bar. The main content area displays the 'Firewall / Schedules' page. A warning message at the top states: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' Below this, the 'Schedules' table is shown with one entry: 'CamGioHanhChinh' with a range of 'October 14 - 20 / 8:00-17:00 /'. The table has columns for Name, Range: Date / Times / Name, Description, and Actions. A green '+ Add' button is at the bottom right.

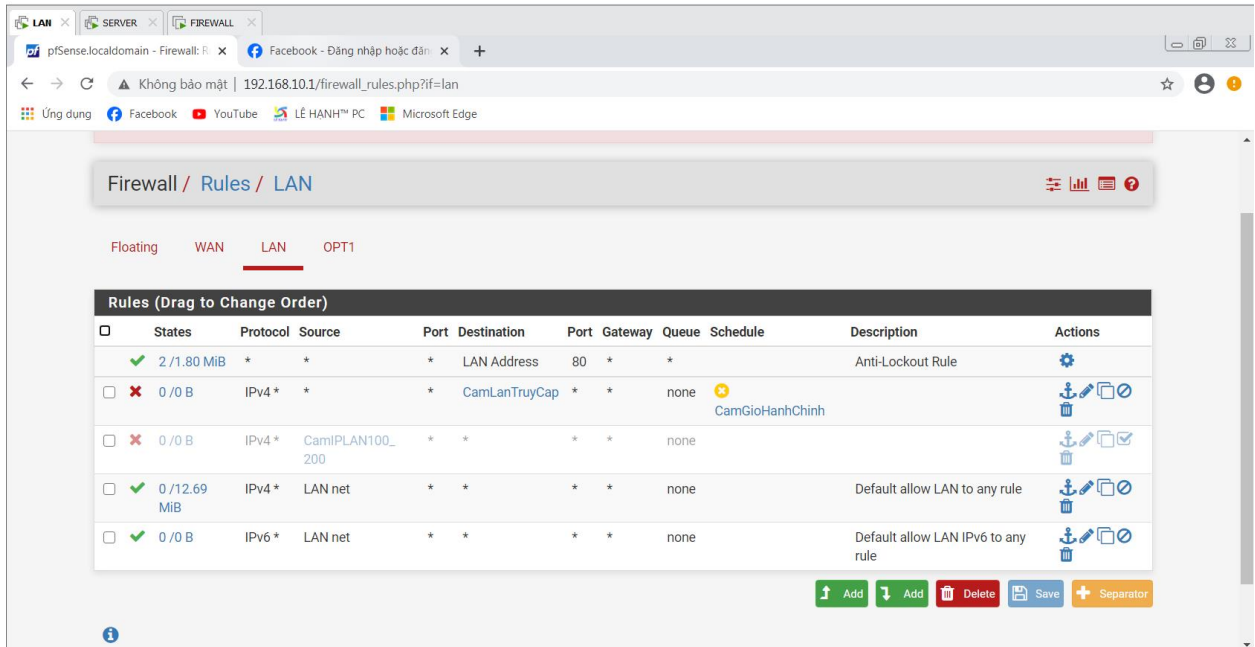
Name	Range: Date / Times / Name	Description	Actions
CamGioHanhChinh	October 14 - 20 / 8:00-17:00 /		



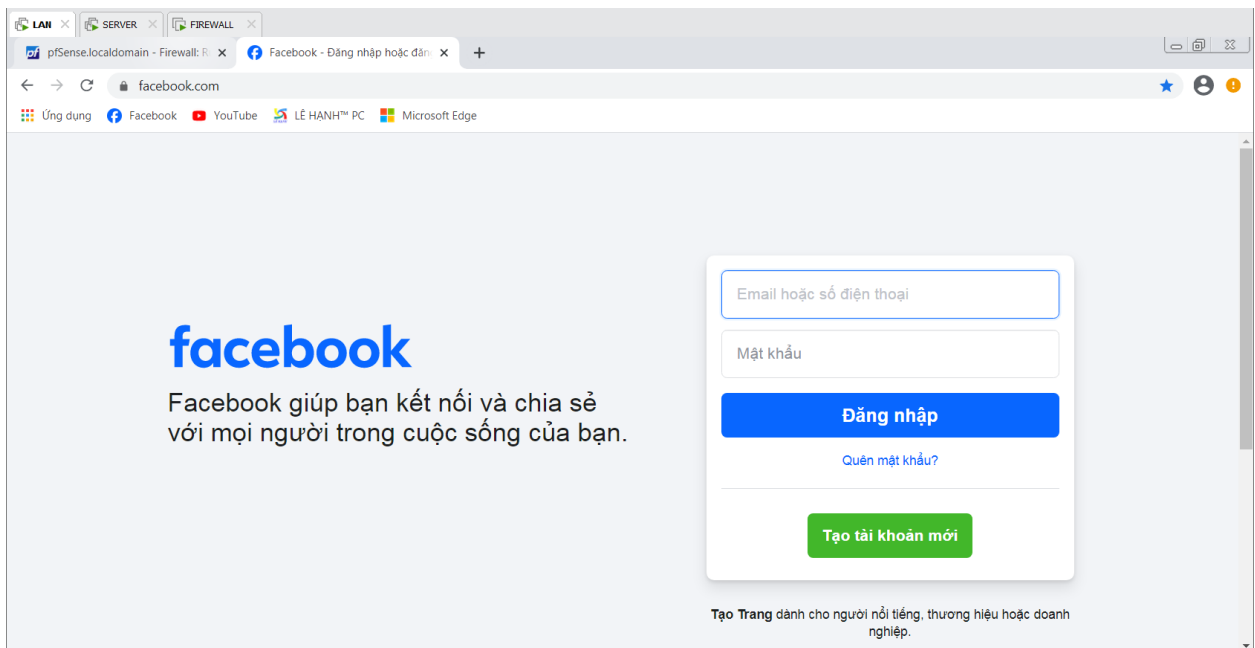
The screenshot shows the pfSense web interface with the 'LAN' tab selected. The main content area displays the 'Firewall / Rules / LAN' page. A green message at the top states: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.' Below this, the 'Rules (Drag to Change Order)' table is shown. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The second rule, 'CamLanTruyCap', is highlighted with a red box. It has a status of '0/2 KIB', protocol of 'IPv4', and schedule of 'CamGioHanhChinh'.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 6 / 1.76 MiB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	
✗ 0 / 2 KIB	IPv4 *	*	*	CamLanTruyCap	*	*	none	CamGioHanhChinh		
✗ 0 / 0 B	IPv4 *	CamPLAN100_200	*	*	*	*	none			
✓ 1 / 12.57 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

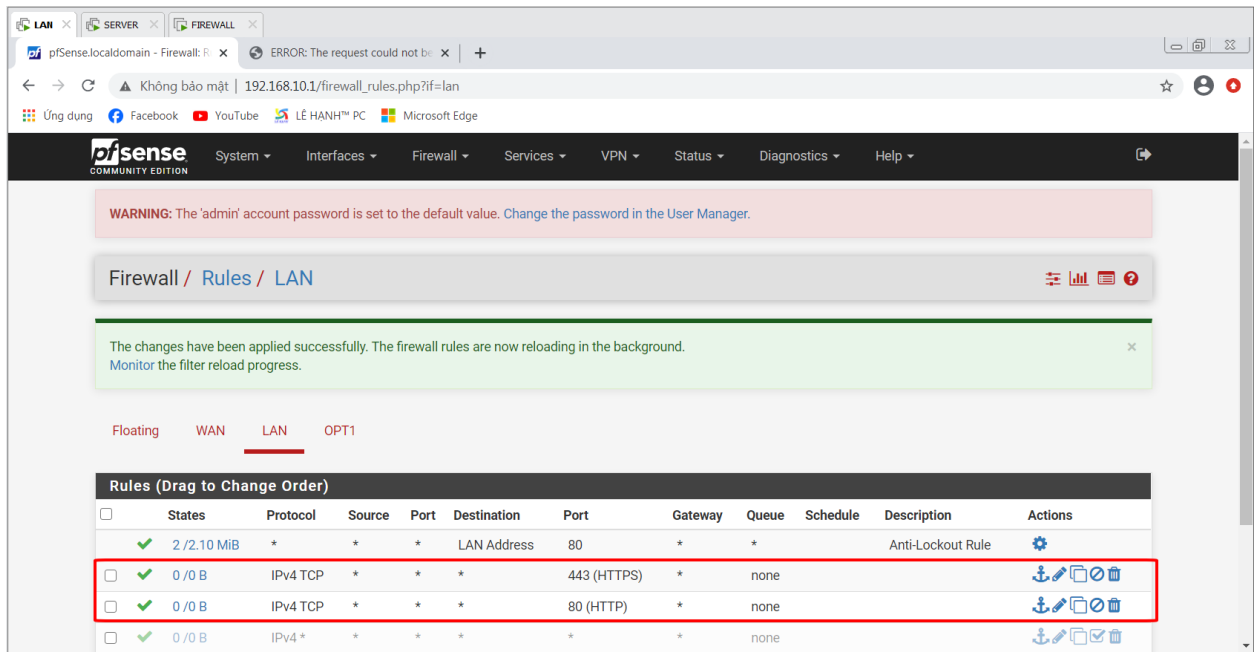
Khi hết giờ



Kiểm tra lại



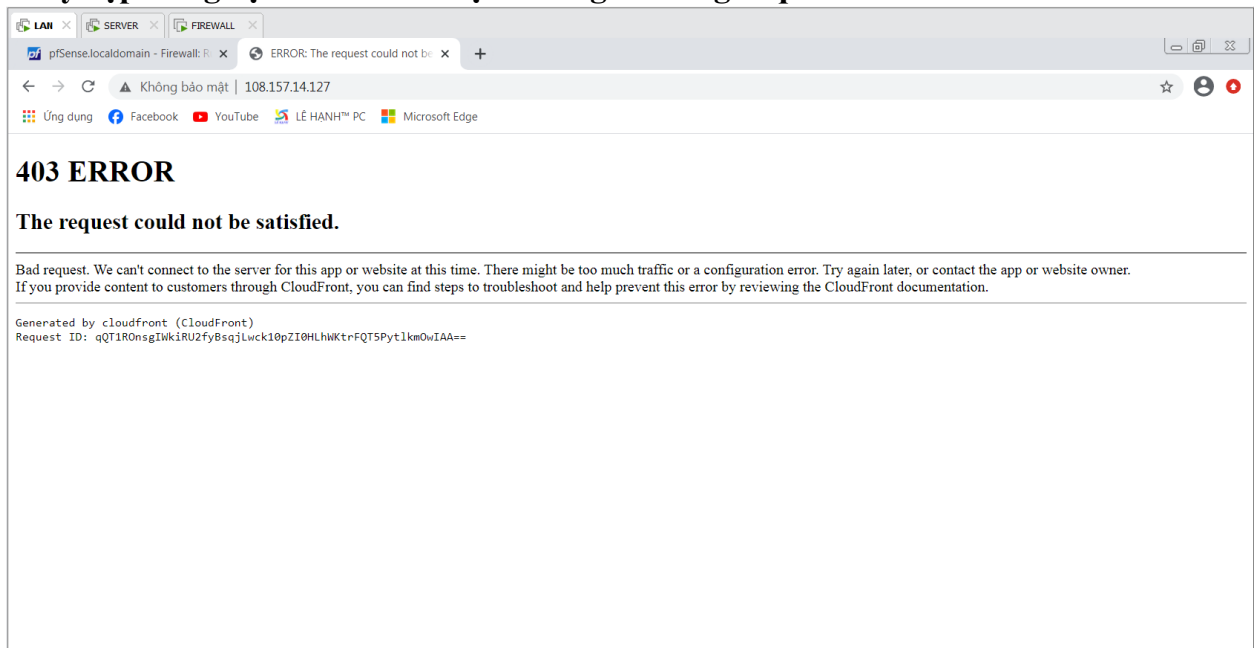
5. Chỉ cho LAN truy cập TCP 80, 443. Kiểm tra LAN chỉ kết nối HTTP bằng IP



The screenshot shows the pfSense Firewall Rules configuration page for the LAN interface. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, a green message indicates that changes have been applied successfully and firewall rules are reloading. The "Rules (Drag to Change Order)" table is displayed with the following data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 / 2.10 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 0 / 0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
✓ 0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
✓ 0 / 0 B	IPv4 *	*	*	*	*	*	none			

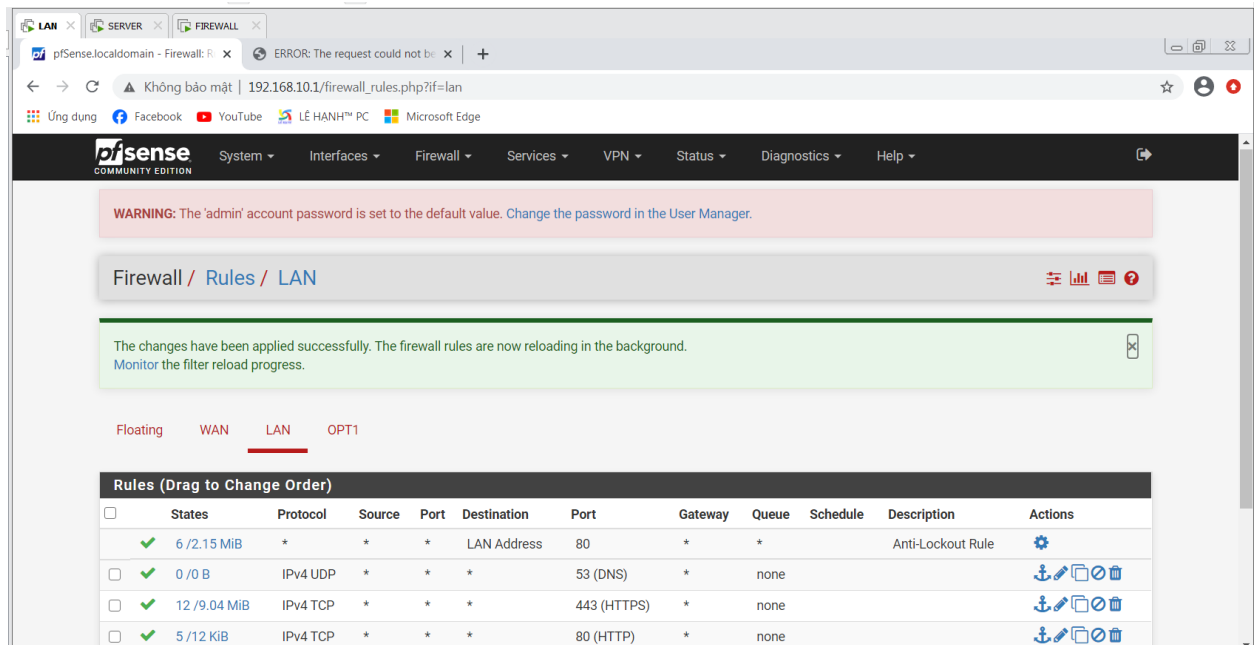
Truy cập bằng địa chỉ IP thì được nhưng lỗi cổng request 403



The screenshot shows a 403 ERROR page. The main heading is "403 ERROR". Below it, the text reads: "The request could not be satisfied." A detailed message follows: "Bad request. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner. If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation." At the bottom, it says "Generated by CloudFront (CloudFront)" and provides a "Request ID: qQT1R0nsgIwkiRU2fyBsqJLwck10pZI0HLhKtrFQT5PytLkm0wIAA==".

6. Mở và chặn DNS tại UDP port 53

Mở cổng



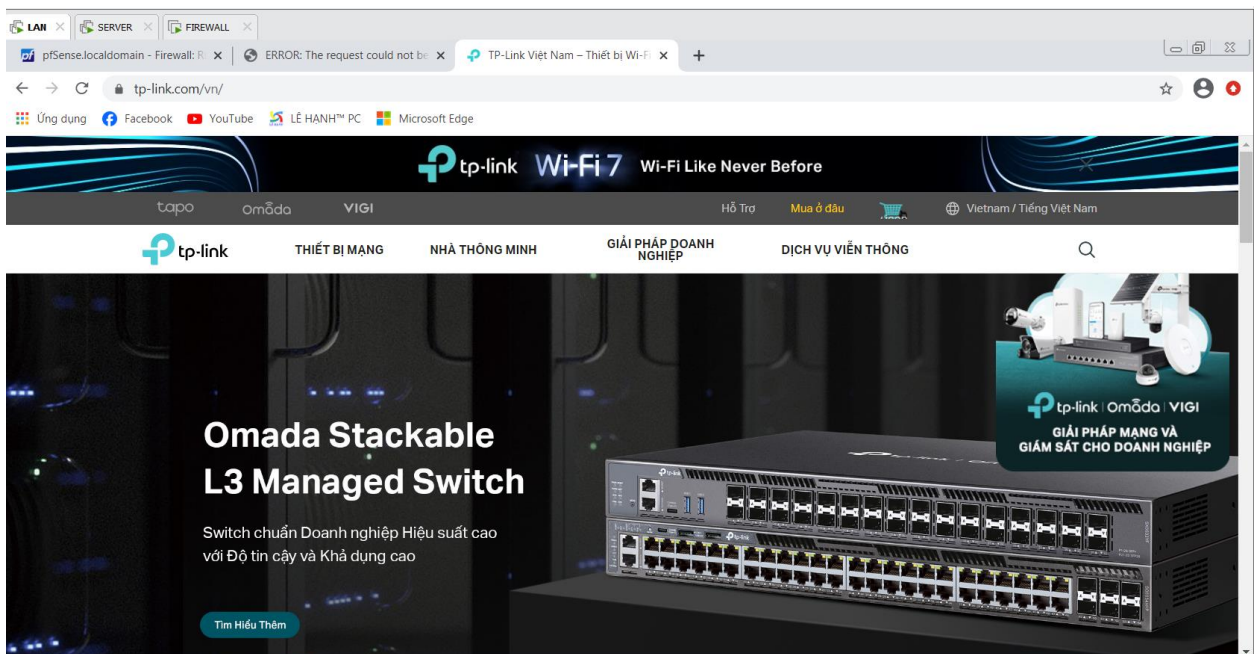
WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background. [Monitor the filter reload progress.](#)

Floating WAN LAN OPT1

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 6 / 2.15 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 12 / 9.04 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 5 / 12 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none			



tp-link Wi-Fi 7 Wi-Fi Like Never Before

tapo omada VIGI Hỗ Trợ Mua ở đâu Vietnam / Tiếng Việt Nam

tp-link THIẾT BỊ MẠNG NHÀ THÔNG MINH GIẢI PHÁP DOANH NGHIỆP DỊCH VỤ VIỄN THÔNG

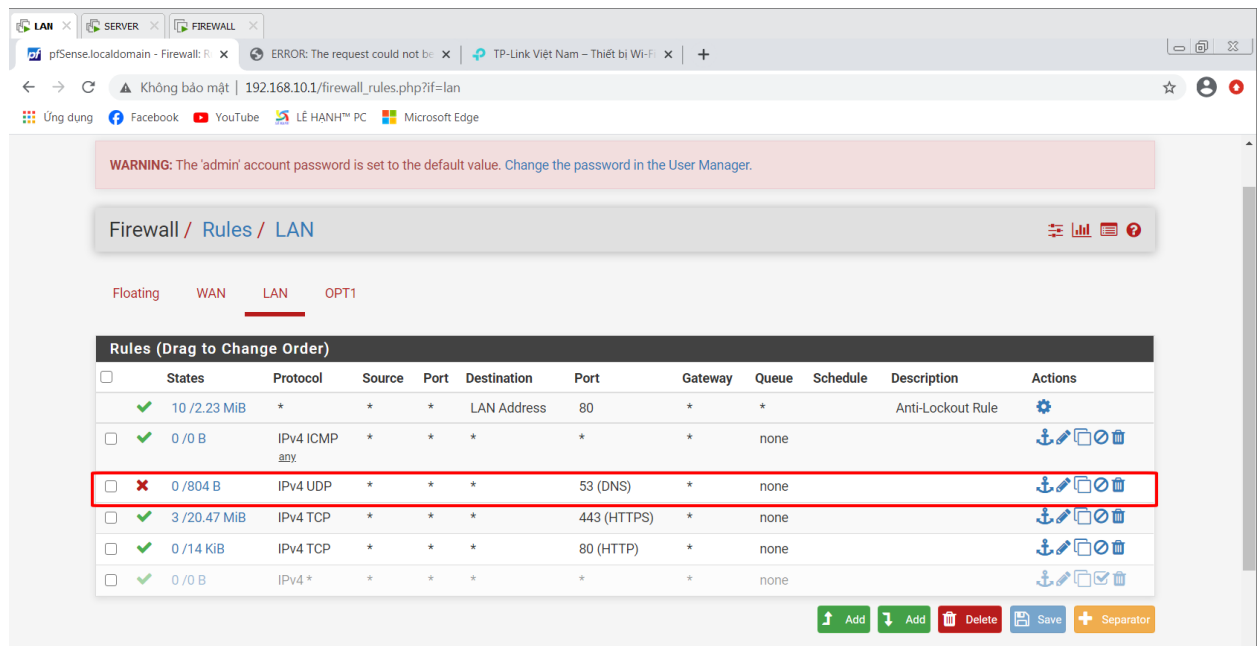
Omada Stackable L3 Managed Switch

Switch chuẩn Doanh nghiệp Hiệu suất cao với Độ tin cậy và Khả dụng cao

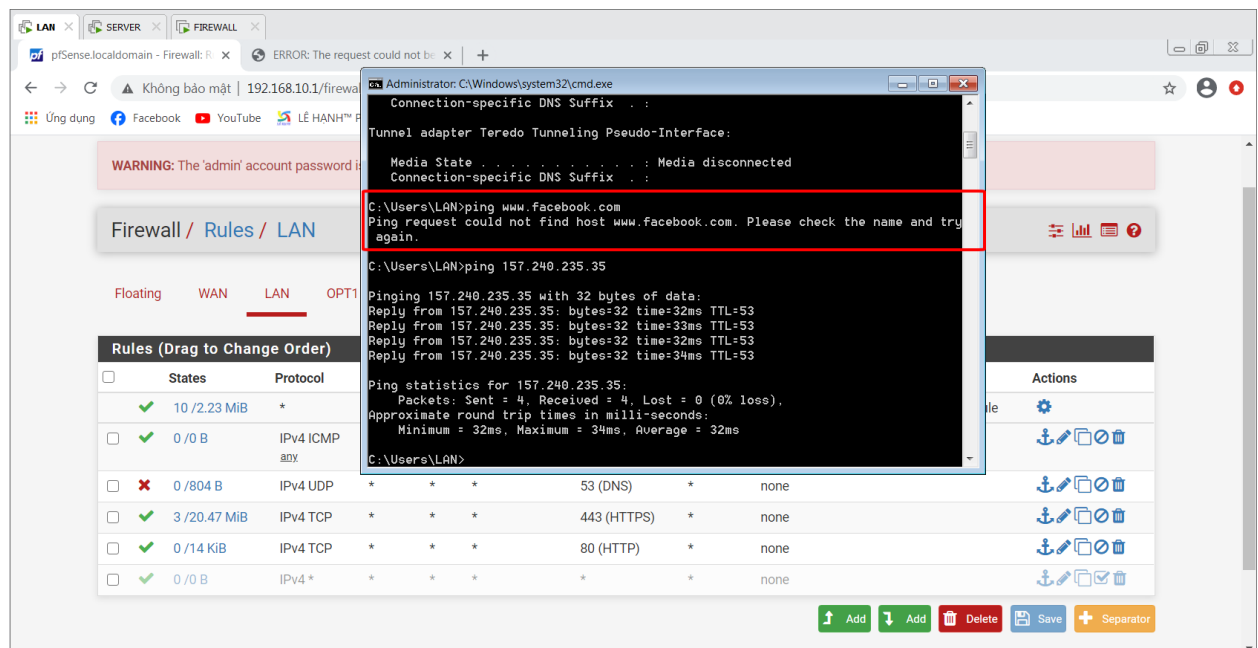
[Tìm Hiểu Thêm](#)

tp-link | Omada | VIGI
GIẢI PHÁP MẠNG VÀ GIÁM SÁT CHO DOANH NGHIỆP

Chặn DNS

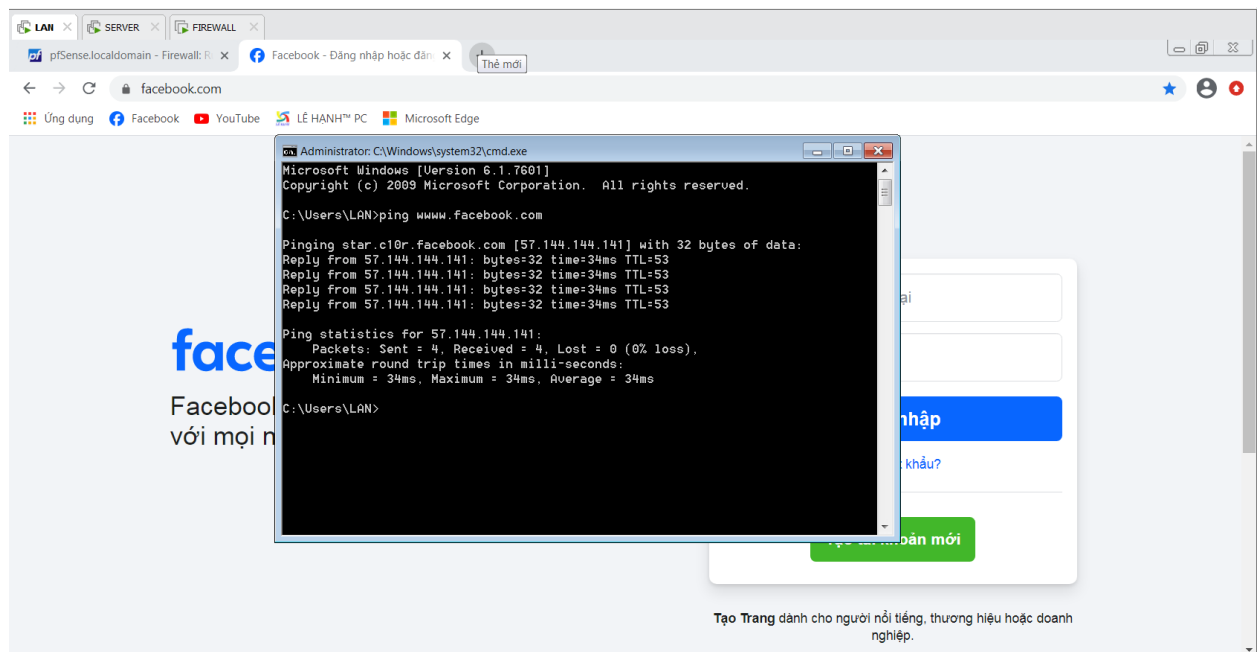


Kết quả là không ping bằng tên miền do không phân giải DNS được và chỉ ping được tới địa chỉ đó

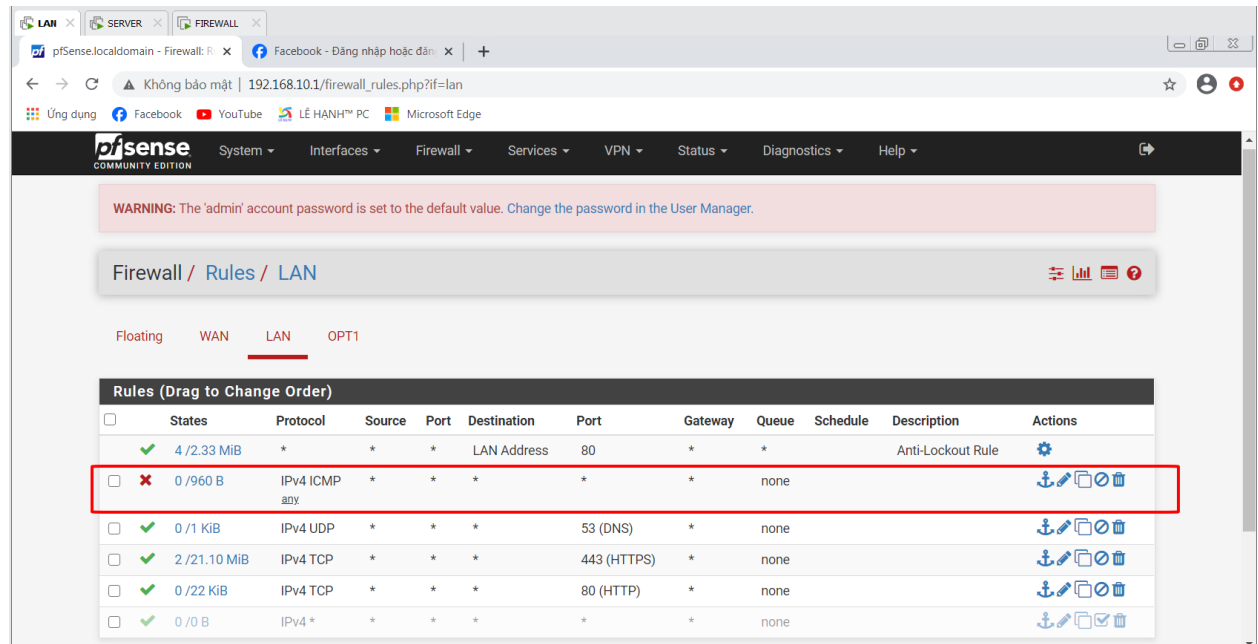


7. Mở và chặn ICMP LAN ping ra Internet

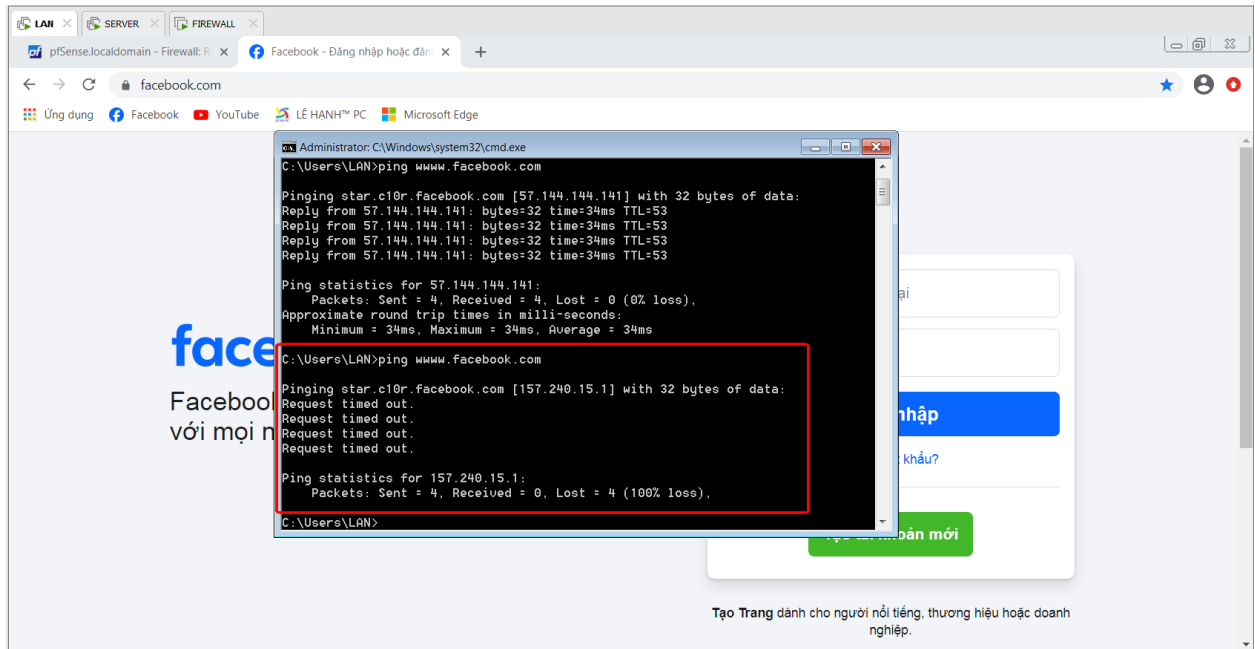
Mở ICMP để ping



Chặn ICMP để không ping được



Kết quả của chặn ICMP là không ping được tới địa chỉ IP mà vẫn truy cập web được



8. Thiết lập DNS, WEB Server tại vùng DMZ

- thiết lập vùng DMZ VMnet3

The image shows two screenshots from a Mikrotik WinBox environment. The top screenshot displays the configuration for the DMZ (em2) interface. A warning message at the top states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The interface configuration is as follows:

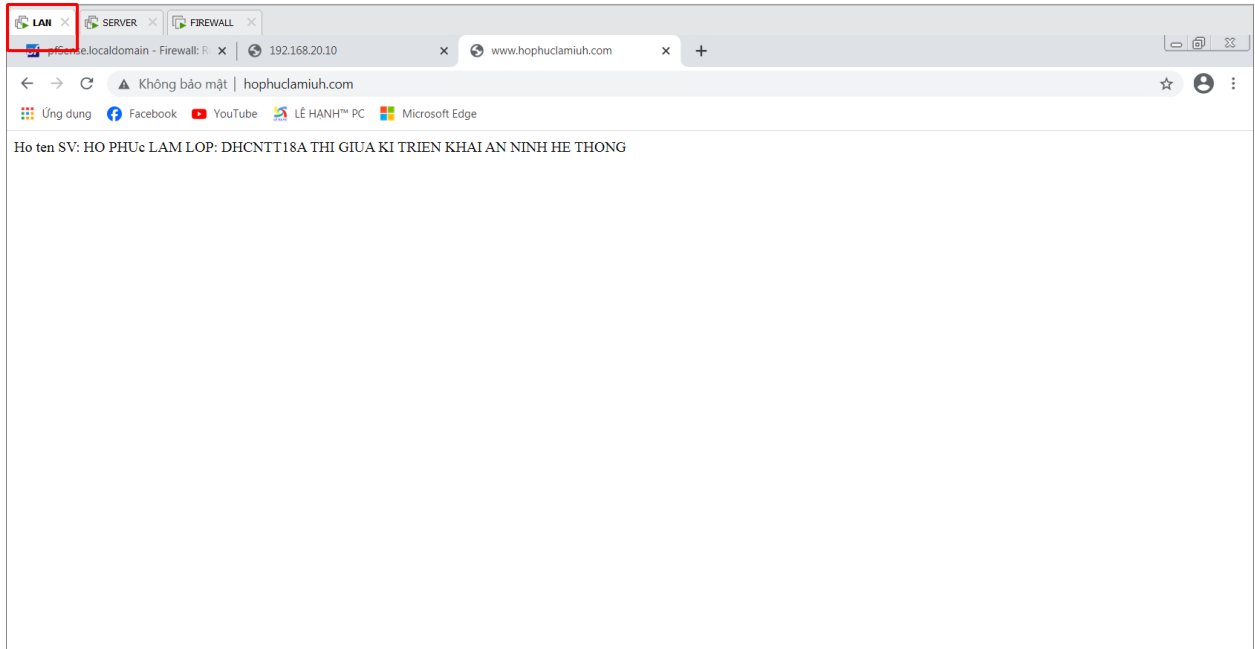
General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	DMZ <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	xxxxxxxxxxxx <small>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx or leave blank.</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.</small>
Speed and Duplex	Default (no preference, typically autoselect) <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.</small>

Below the general configuration is the Static IPv4 Configuration section:

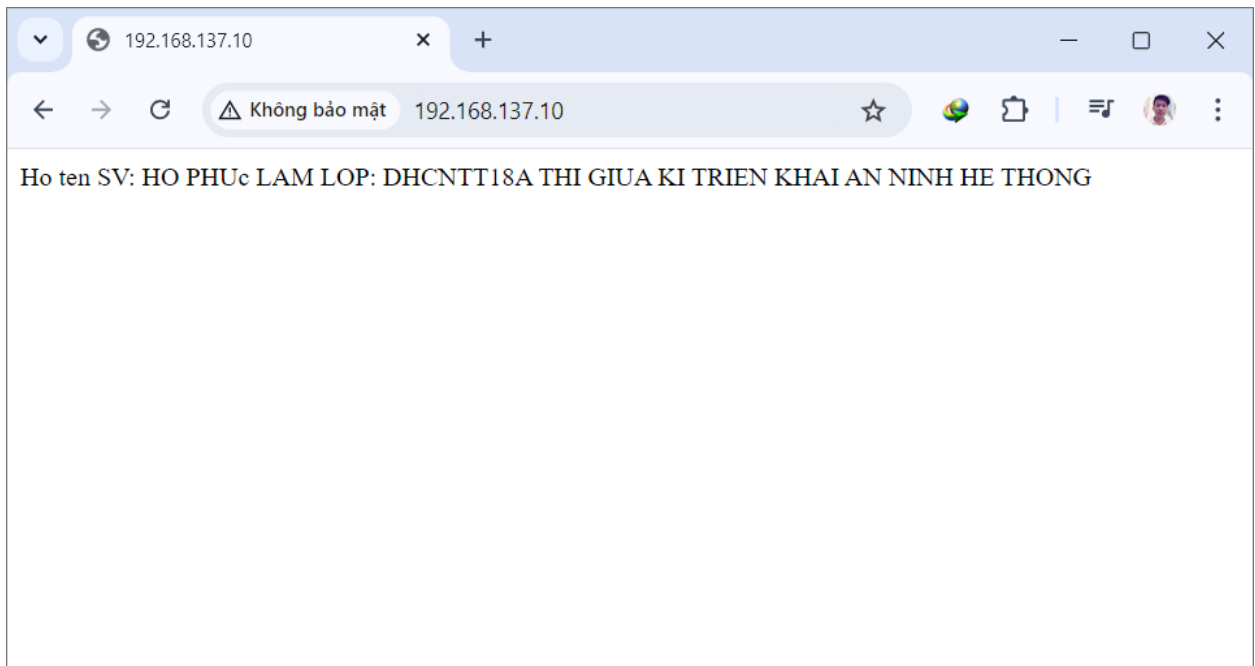
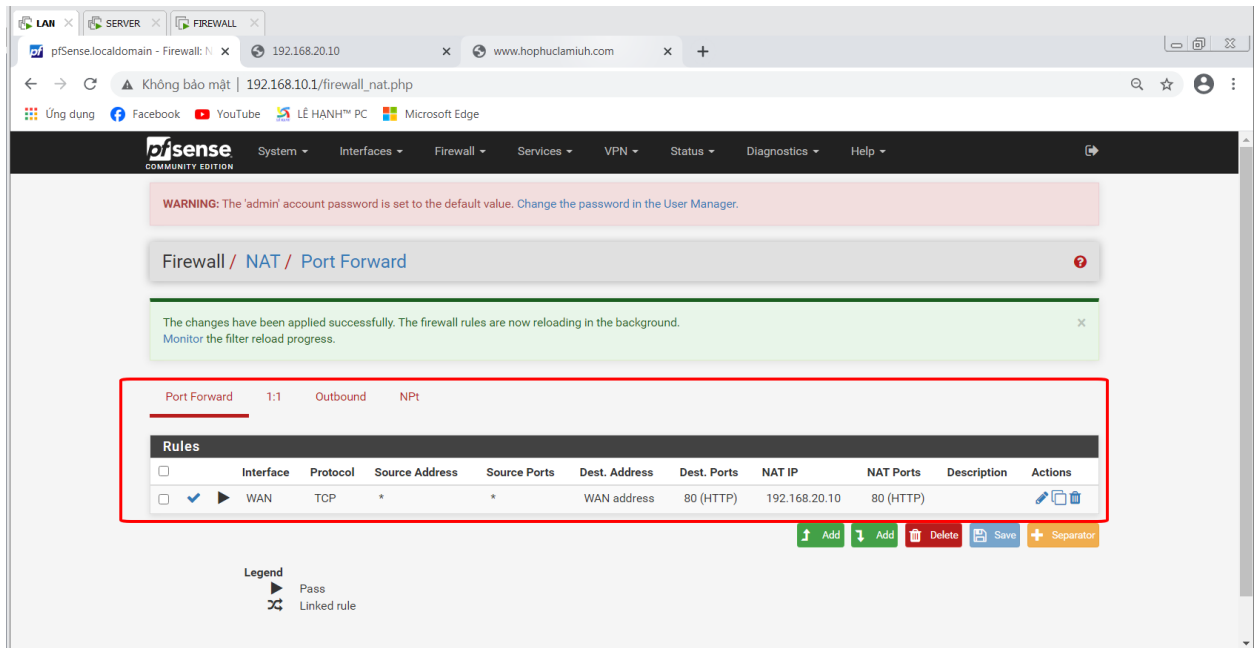
Static IPv4 Configuration	
IPv4 Address	192.168.20.1 / 24

The bottom screenshot shows a Windows Internet Explorer browser window with the address bar set to <http://www.hophudamiuh.com/>. The page content displays the text: "Họ tên SV: HO PHUC LAM LOP: DHCNTT18A THI GIUA KI TRIEN KHAI AN NINH HE THONG". The browser's status bar at the bottom indicates "Done" and "Internet | Protected Mode: Off".

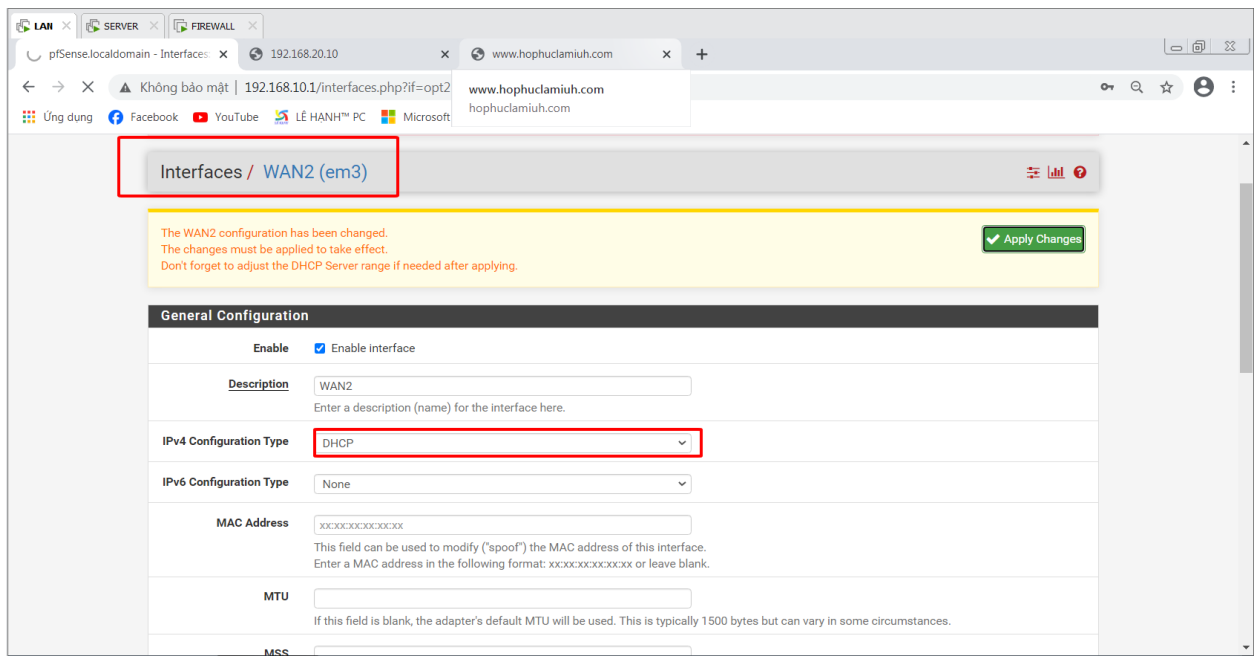
LAN đã truy cập được DMZ



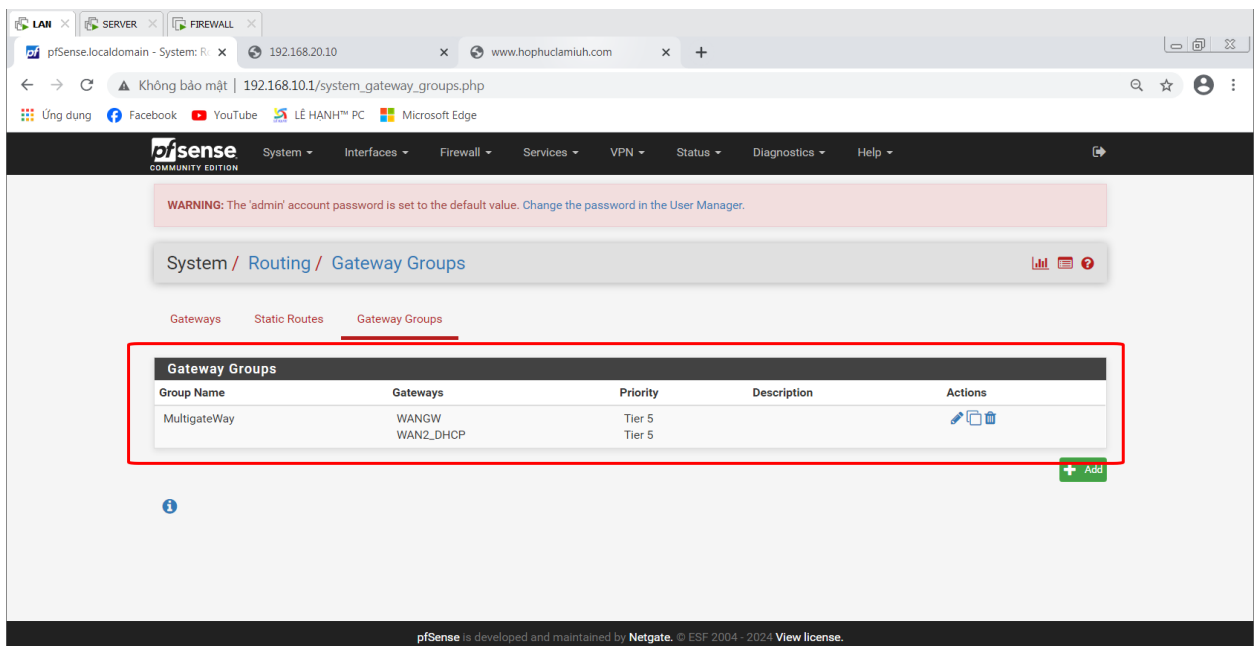
9. Public WEB Server



10. Cấu hình MultiGateway WAN1, WAN2 để dự phòng mất kết nối Internet.



Cấu hình routing để làm dự phòng



LAN x SERVER x FIREWALL x

pfSense.localdomain - System: R... x 192.168.20.10 x www.hophuclamuih.com x +






Không bảo mật | 192.168.10.1/system_gateways.php



Ứng dụng Facebook YouTube LÊ HANH™ PC Microsoft Edge

System / Routing / Gateways

The changes have been applied successfully.

Gateways Static Routes Gateway Groups


Gateways							
	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input type="checkbox"/>	WANGW	Tier 5 (IPv4)	WAN	192.168.137.1	192.168.137.1	Interface wan Gateway	  
<input checked="" type="checkbox"/>	WAN2_DHCP	Tier 5 (IPv4)	WAN2	192.168.153.2	192.168.153.2	Interface WAN2_DHCP Gateway	 

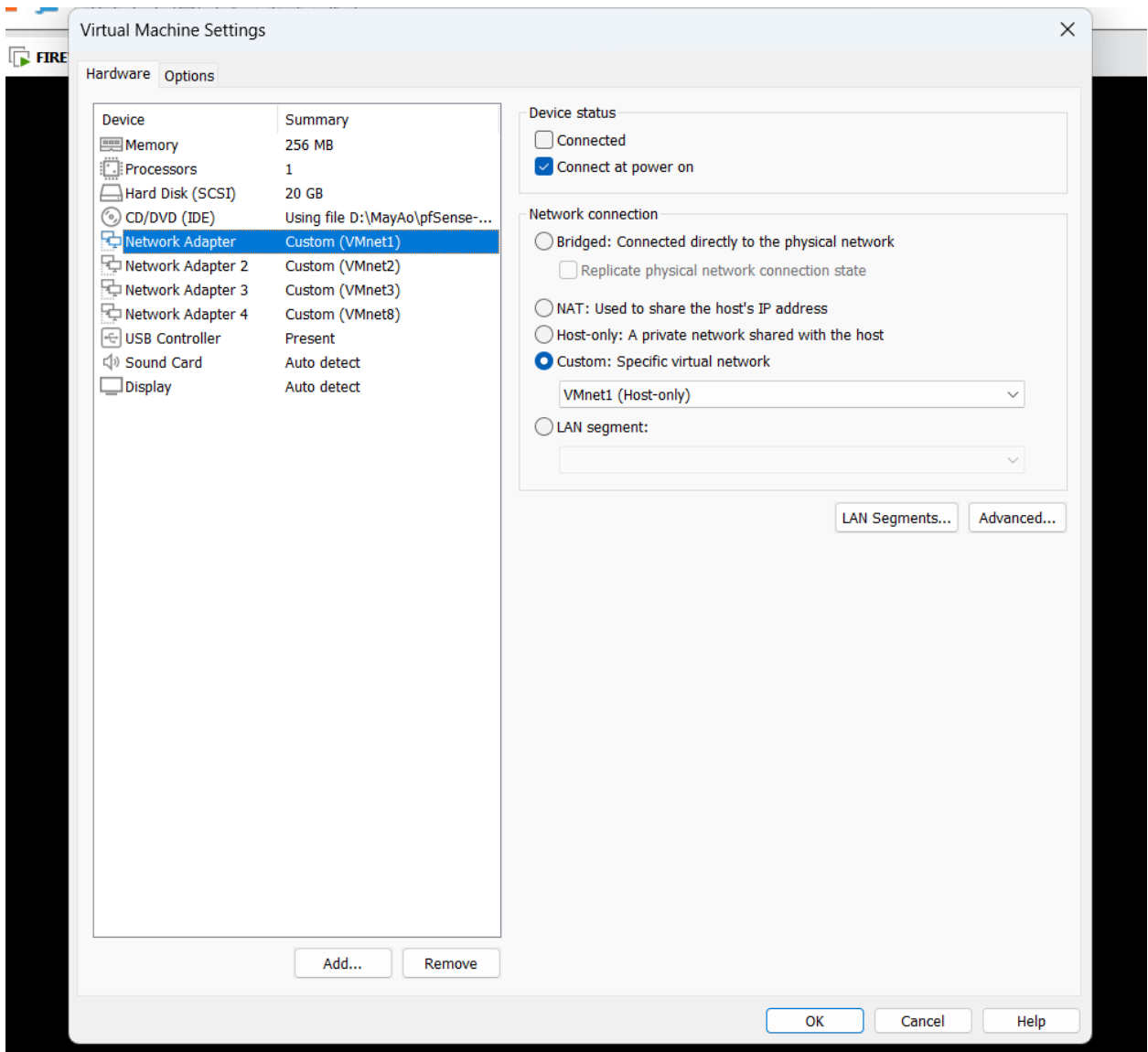
Default gateway

Default gateway IPv4
Select the gateway or gatewaygroup to use as the default gateway.

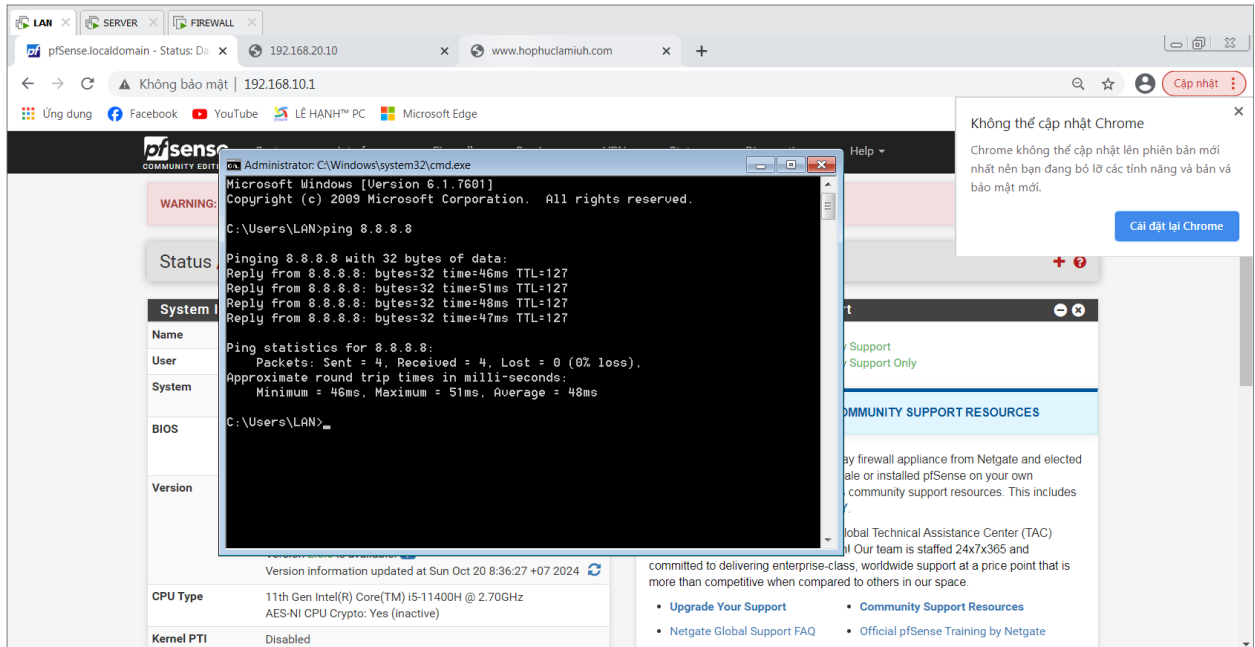
Default gateway IPv6
Select the gateway or gatewaygroup to use as the default gateway.



Kiểm tra bằng các tắt VMnet1 của WAN



Kết quả là nó chuyển sang VMnet8 và vẫn truy cập đc internet

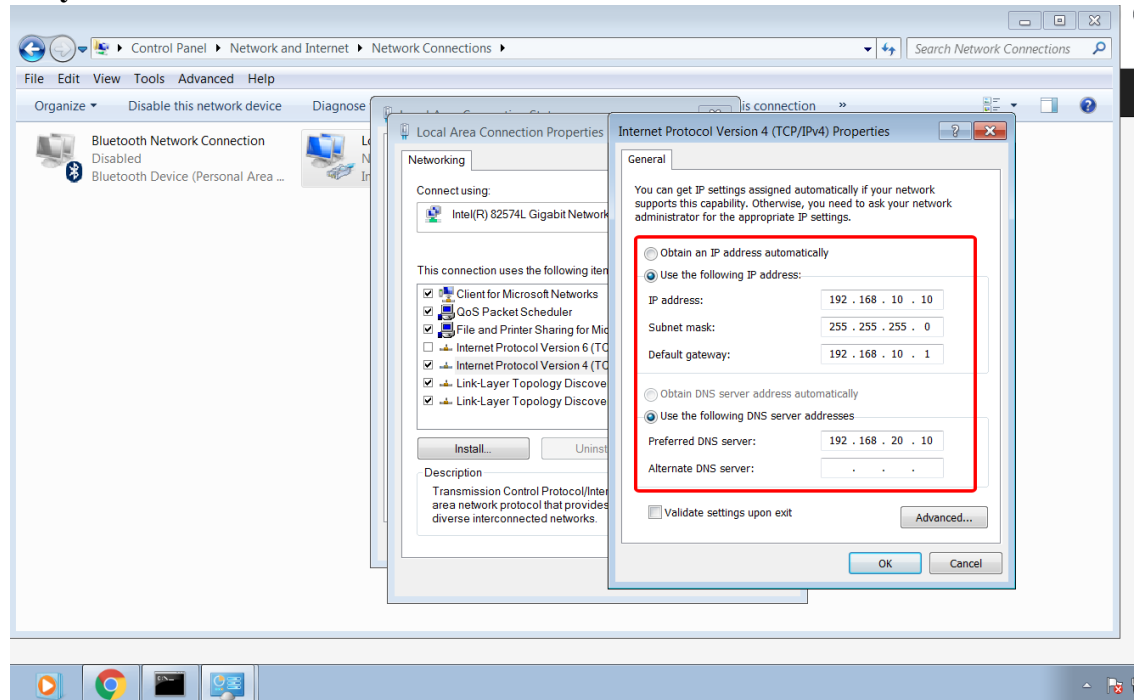


---Kết thúc bài lab---

Làm chi tiết các bước

1. Cấu hình máy LAN DMZ SERVER

a. Máy LAN



b.

c. Firewall

```
Enter an option:

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 3bc3497d303a4009b52a

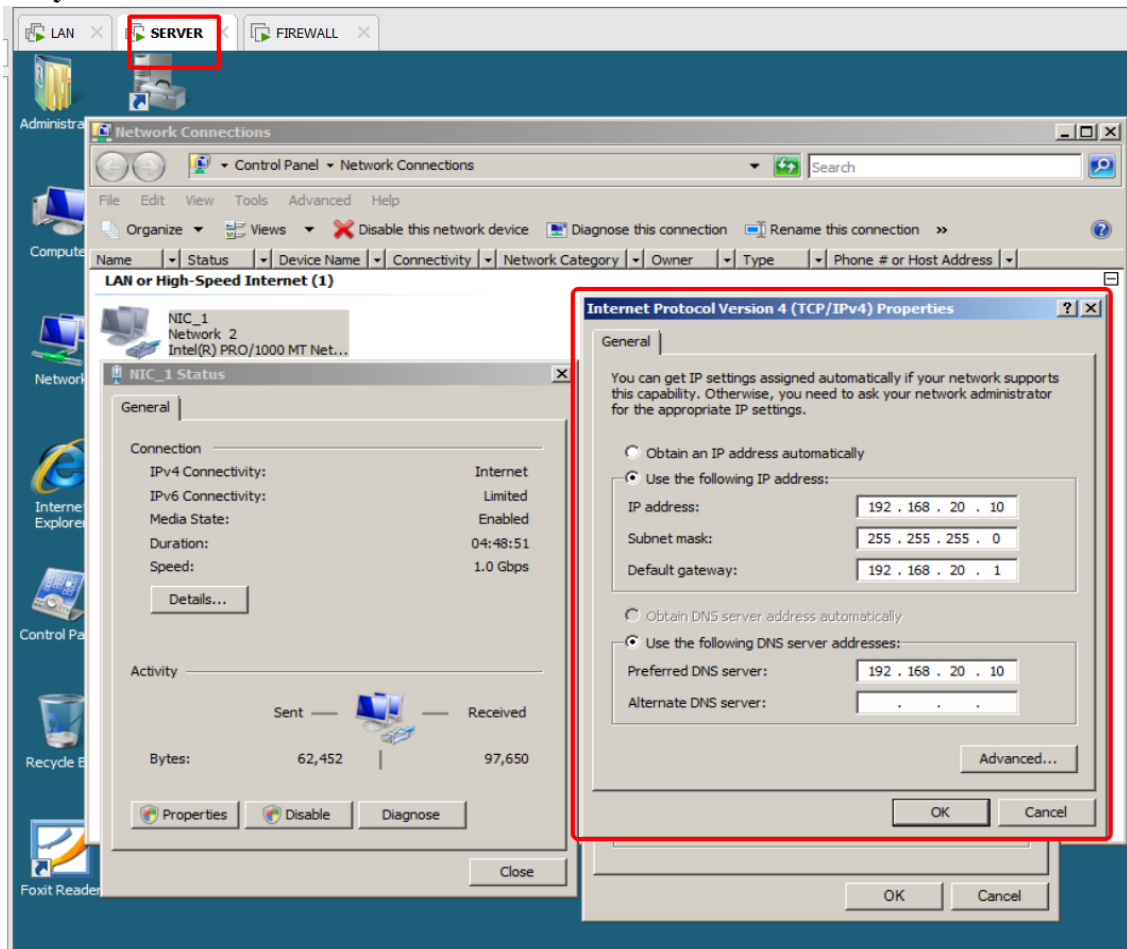
*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.137.10/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 192.168.20.1/24
WAN2 (opt2)    -> em3      -> v4/DHCP4: 192.168.153.128/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

d. Máy server



e. Mạng VMnet

The screenshot shows the 'Virtual Network Editor' window. At the top, there is a table listing several VMnets. Below the table are buttons for 'Add Network...', 'Remove Network', and 'Rename Network...'. The 'VMnet Information' section is expanded, showing three radio button options: 'Bridged', 'NAT', and 'Host-only'. The 'Host-only' option is selected. Below these options, there is a checkbox for 'Connect a host virtual adapter to this network' which is checked, and a text field for 'Host virtual adapter name' containing 'VMware Network Adapter VMnet1'. There is also a checkbox for 'Use local DHCP service to distribute IP address to VMs' which is unchecked. At the bottom of the configuration section, there are input fields for 'Subnet IP' (192.168.187.0) and 'Subnet mask' (255.255.255.0). A warning message at the bottom states 'Administrator privileges are required to modify the network configuration.' with a 'Change Settings' button. At the very bottom, there are buttons for 'Restore Defaults', 'Import...', 'Export...', 'OK', 'Cancel', 'Apply', and 'Help'.

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	-	192.168.187.0
VMnet2	Host-only	-	Connected	-	192.168.61.0
VMnet3	Host-only	-	Connected	-	192.168.93.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.238.0

Buttons: Add Network..., Remove Network, Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)
Bridged to: Automatic Settings...

☐ NAT (shared host's IP address with VMs)
NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☒ Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet1

☐ Use local DHCP service to distribute IP address to VMs
DHCP Settings...

Subnet IP: Subnet mask:

⚠ Administrator privileges are required to modify the network configuration. [Change Settings](#)

Buttons: Restore Defaults, Import..., Export..., OK, Cancel, Apply, Help

