

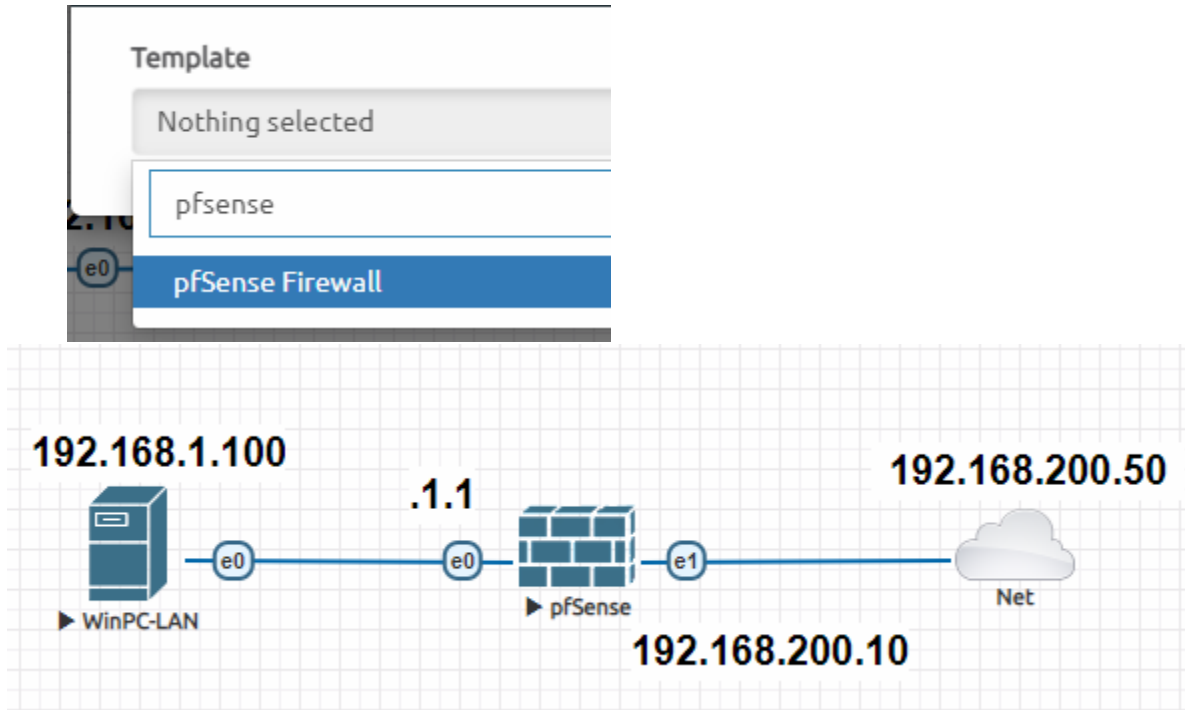
CẤU HÌNH PFSENSE CƠ BẢN CHO NGƯỜI MỚI-Verion 2

- 1 Cài đặt PFSENSE vào EVE-NG
- 2 Đặt IP cho interface và ra internet
- 3 Tạo user cho firewall
- 4 Cấu hình DHCP server
- 5 Cấu hình chặn mở truy cập
- 6 BACKUP và RESTORE
- 7 Đặt policy theo thời gian
- 8 Upgrade OS cho firewall
- 9 Cấu hình Port forwarding
- 10 Static NAT
- 11 Cài gói OSPF và Cấu hình OSPF

<https://hainguyenit.edubit.vn>

1. Cài đặt PFSENSE vào EVE-NG

- Vào download bản pfsense cho eve tại đây:
https://mega.nz/folder/2AVXDTYR#B_A8m89hvJbkeHyGCAbx7w/folder/yBsEAazJ
- Vào eve tạo thư mục `/opt/unetlab/addons/qemu/pfsense-CE-2.3` và đẩy file pfsense vừa down ở trên vào
- Vào giao diện web của eve, tạo bài lab mới và chuột phải chọn add node pfsense:



2. Đặt ip cho interface và ra internet

Kích đúp vào node vừa tạo để mở màn hình putty hoặc secureCRT như dưới:

```
If you do not know the names of the interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.
```

```
Enter the WAN interface name or 'a' for auto-detection (vtnet0 vtnet1 or a):
```

Gõ vtnet1 cho WAN , vtnet0 cho LAN (tương ứng cổng e1 và e0)

```
The interfaces will be assigned as follows:
```

```
WAN -> vtnet1  
LAN -> vtnet0
```

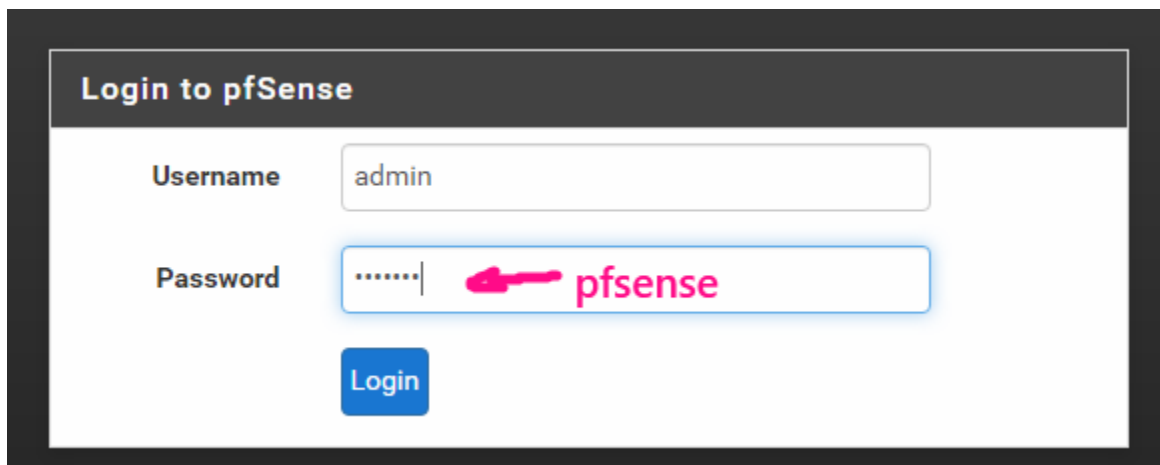
```
Do you want to proceed [y|n]? y
```

https://hainguyenit.edubit.vn

```
*** Welcome to pfSense 2.3-RELEASE-pfSense (amd64) on pfSense ***  
WAN (wan)      -> vtnet1      ->  
LAN (lan)      -> vtnet0      -> v4: 192.168.1.1/24  
  
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) pfSense Developer Shell  
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:

Sau đó vào trình duyệt PC- đấu nối với PfSense, gõ 192.168.1.1

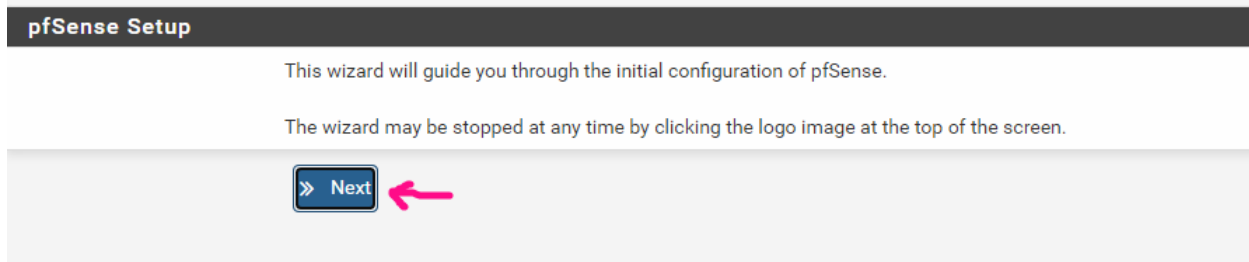


Login to pfSense

Username: admin

Password: pfsense

Login



pfSense Setup

This wizard will guide you through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

» Next

General Information

On this screen the general pfSense parameters will be set.

Hostname	<input type="text" value="my-lab"/>
	EXAMPLE: myserver
Domain	<input type="text" value="local.local"/>
	EXAMPLE: mydomain.com
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text"/>
Override DNS	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

Time Server Information

Please enter the time, date and time zone.

Time server hostname	<input type="text" value="0.pfsense.pool.ntp.org"/>
	Enter the hostname (FQDN) of the time server.
Timezone	<input type="text" value="Asia/Bangkok"/>

[» Next](#)

Đặt IP cho WAN theo mô hình

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType	<input type="text" value="Static"/>
--------------	-------------------------------------

https://hainguyenit.edubit.vn

Static IP Configuration

IP Address	<input type="text" value="192.168.200.10"/>
Subnet Mask	<input type="text" value="24"/>
Upstream Gateway	<input type="text" value="192.168.200.50"/>

DHCP client configuration

Bấm NEXT

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	<input type="text" value="192.168.1.1"/>
Subnet Mask	<input type="text" value="24"/>

Type dhcp if this interface uses DHCP to obtain its IP address.

Khi setup LAN, WAN xong là firewall sẽ tự NAT từ LAN đi ra mạng
Bước cuối reboot pfSense để apply các cấu hình là xong phần đi internet

Reload configuration

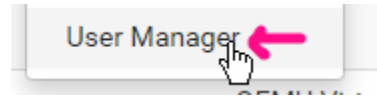
Click 'Reload' to reload pfSense with new chan


Check lại trên PC: vào 24h.com.vn

https://hainguyenit.edubit.vn

3. Tạo user mới cho firewall và giới hạn quyền

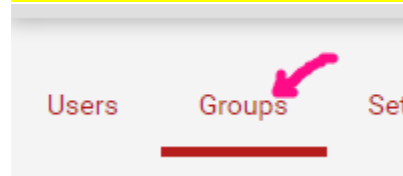
Vào system > User manager



Chọn Add,  rồi điền thông số. Ví dụ ở đây tôi tạo 1 user tên là hainm và thuộc nhóm thực tập sinh, chỉ có quyền xem 1 vài page trên trang quản trị firewall

Username	<input type="text" value="hainm"/>	
Password	<input type="password" value="Password"/>	<input type="password" value="Confirm Password"/>
Full name	<input type="text"/>	User's full name, for administrative information only
Expiration date	<input type="text" value="mm/dd/yyyy"/>	Leave blank if the account shouldn't expire, otherwise enter the expiration date
Membership	<input type="text" value="admins"/>	<input type="text" value="thuctap"/>
	Not member of	Member of
	» Move to "Member of" list	« Move to "Not member of" list

Tạo nhóm "Thực tập" và set quyền:



Chọn ADD

Group Properties	
Group name	<input type="text" value="thuctap"/>
Scope	<input type="text" value="Local"/>
Description	<input type="text"/>

Rồi set các page mà user này được vào

https://hainguyenit.edubit.vn

Assigned Privileges	
Name	Description
WebCfg - All pages	Allow access to all pages
WebCfg - Firewall: Rules	Allow access to the 'Firewall: Rules' page.

Quay lại tab user để gán user hainm vào nhóm ThucTap

Group membership

admins
thuctap

Not member of

Member of

>> Move to "Member of" list

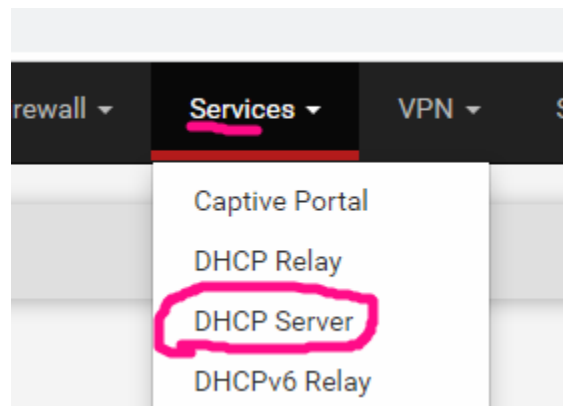
<< Move to "Not member of" list

Hold down CTRL (pc)/COMMAND (mac) key to select multiple items

Save và Thoát ra và test lại đăng nhập bằng user hainm

4. Cấu hình DHCP server

Vào Service > DHCP server



Kiểm tra mục General Option đã được điền sẵn, có thể chỉnh IP range theo ý mình

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
Deny unknown clients	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	<input type="text" value="192.168.1.10"/> <input type="text" value="192.168.1.245"/>

https://hainguyenit.edubit.vn

Điền thêm 1 số thông số cần thiết như gateway, DNS server

Servers

WINS servers	WINS Server 1
	WINS Server 2
DNS servers	8.8.8.8
	DNS Server 2
	DNS Server 3
	DNS Server 4

Leave blank to use the system default DNS : configured on the General page

Other Options

Gateway	192.168.1.1
	The default is to use the IP on this interface network. Type "none" for no gateway assign
Domain name	local.local
	The default is to use the domain name of th

Save lại và vào PC , chọn cho nhận DHCP rồi check đã nhận IP đúng range và gateway và DNS đúng.

IPv4 Address	192.168.1.10
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, May 26, 2022 3:56:38 AM
Lease Expires	Thursday, May 26, 2022 5:56:37 AM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	8.8.8.8

https://hainguyenit.edubit.vn

5. Cấu hình chặn/mở truy cập

Pfsense default rule : allow dải LAN đi all, và cấm all từ wan vào

Ví dụ tôi cần cấm các máy trong LAN đi đến trang web 24h.com.vn (nhiều ip trong dải là 125.212.247.0/24)

Vào Firewall => Rule => Lan => Kịch Add

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✓ 7/4.88 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout
✓ 335/74.72 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow
0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow

2 ↑ Add

Edit Firewall Rule

Action Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP por whereas with block the packet is dropped silently. In either case, the original packet is discarde

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN

Destination

Destination Network 125.212.247.0 / 24

Destination port range Custom any Custom
Sort range for this rule. The "To" field may be left empty if only filtering a single port.

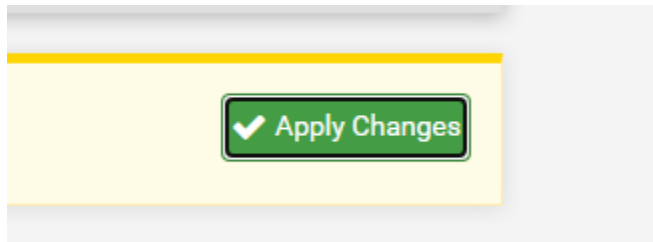
Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everytl the [Status: System Logs: Settings page](#)).

Description

https://hainguyenit.edubit.vn

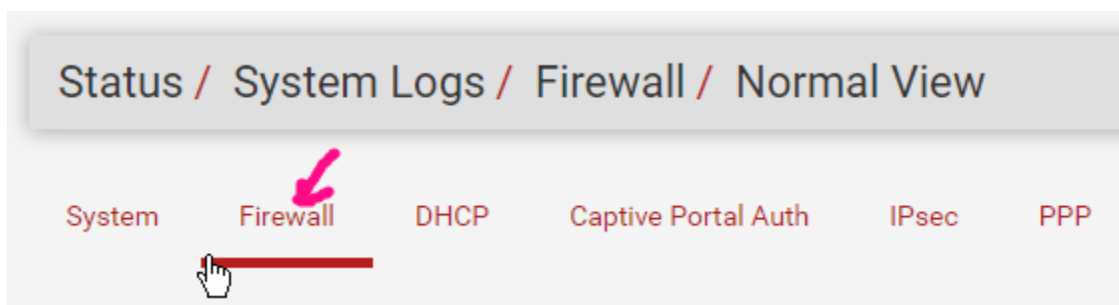
Bấm Save để lưu lại, rồi bấm Apply Change



Verify:

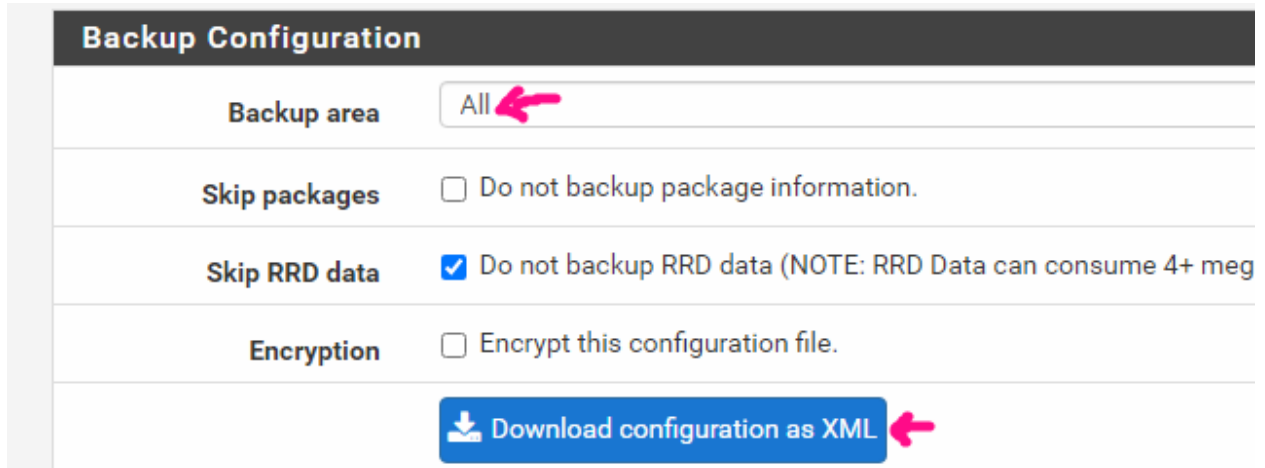
Vào lại trang 24h.com.vn xem tạch chưa

Để xem log drop, ta vào Status > System Log > Firewall:



6. BACKUP và RESTORE cấu hình

Để backup ta vào Diagnostic > Backup & Restore



https://hainguyenit.edubit.vn

Để Restore cấu hình , ta vào mục restore như dưới

Restore Backup

Open a pfSense configuration XML file and click the button below to restore the c

Restore area All

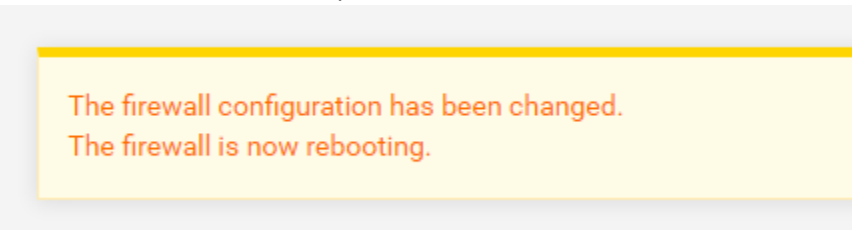
Configuration file Choose File config-my-la...6135514.xml

Encryption Configuration file is encrypted.

Restore Configuration

The firewall will reboot after restoring the configuration.

Sau đó firewall sẽ reboot và phục hồi cấu hình:



7. Đặt policy theo thời gian

Vào Firewall > Schedules , sau đó chỉ ra thời điểm.

Vào Firewall > Rule > kích vào rule cần chọn thời gian có tác dụng, bấm vào hình bút để sửa, kéo xuống dưới chọn Schedules vừa tạo

Extra Options

Log Log packets that are handled by
Hint: the firewall has limited local l... the Status: System Logs: Settings p

Description
A description may be entered here f

Advanced Options

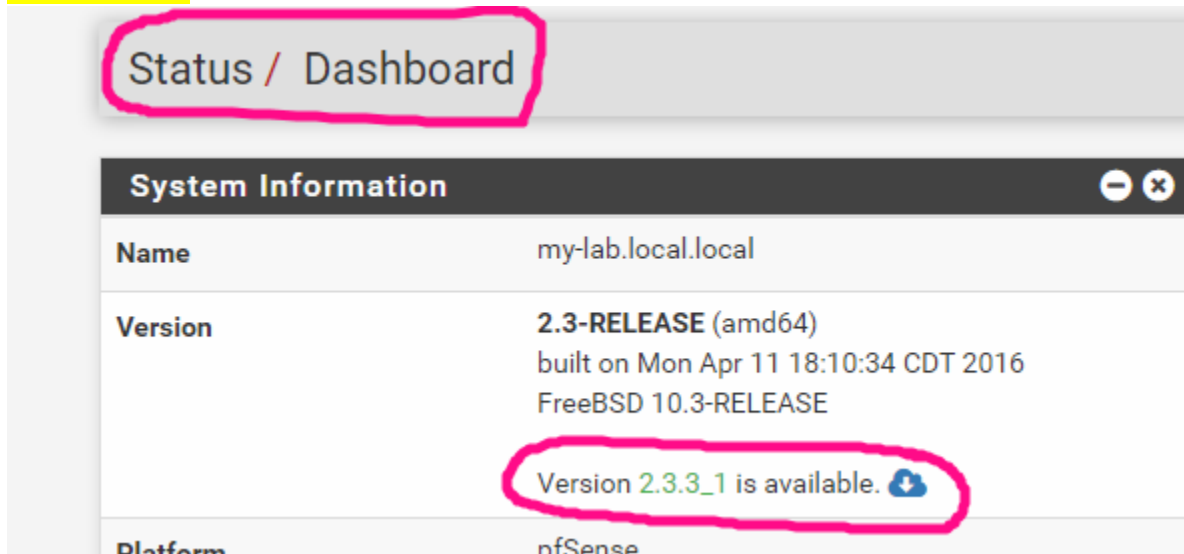
Choose 802.1p priority to apply

Schedule none
none
block_t7
default

Gateway default

8. Update OS cho firewall

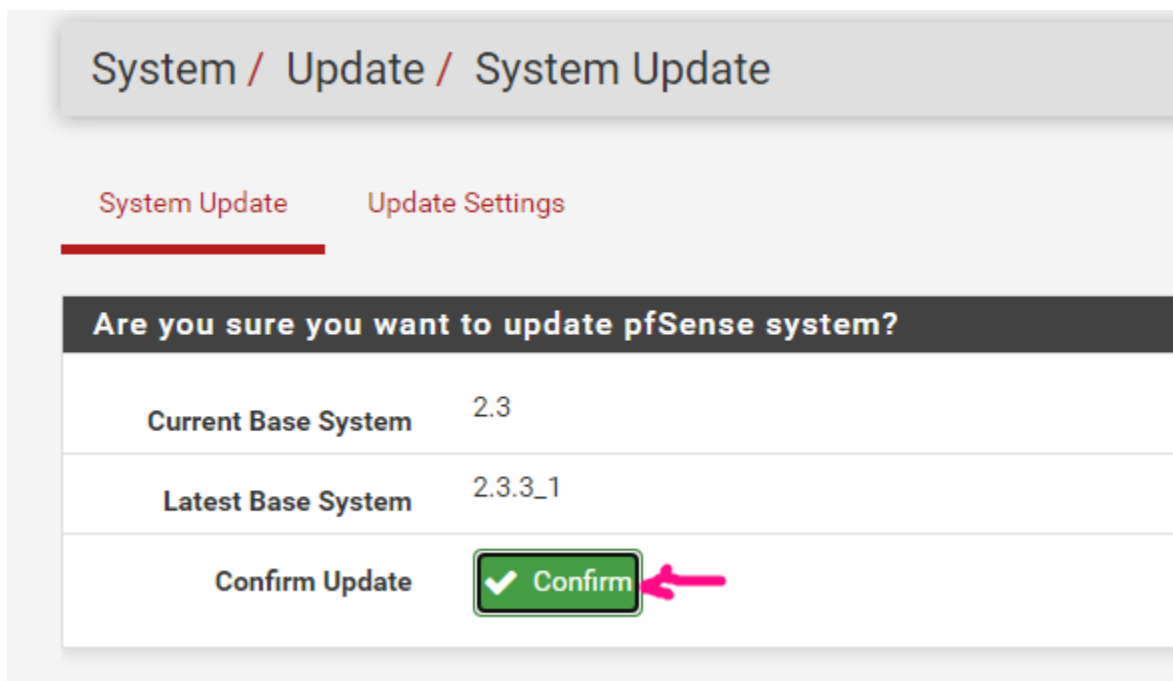
Vào Dashboard



The screenshot shows the 'System Information' window in the pfSense dashboard. The title bar reads 'Status / Dashboard'. The window contains a table with the following information:

Name	my-lab.local.local
Version	2.3-RELEASE (amd64) built on Mon Apr 11 18:10:34 CDT 2016 FreeBSD 10.3-RELEASE
Platform	nfSense

At the bottom of the version information, there is a notification: 'Version 2.3.3_1 is available.' with a download icon. This notification is circled in pink.



The screenshot shows the 'System Update' page in the pfSense dashboard. The title bar reads 'System / Update / System Update'. There are two tabs: 'System Update' (active) and 'Update Settings'. Below the tabs is a confirmation dialog with the title 'Are you sure you want to update pfSense system?'. The dialog contains the following information:

Current Base System	2.3
Latest Base System	2.3.3_1
Confirm Update	<input checked="" type="checkbox"/> Confirm

A pink arrow points to the 'Confirm' button.

Đợi 1 lúc để firewall khởi động xong và check lại OS đã lên version mới

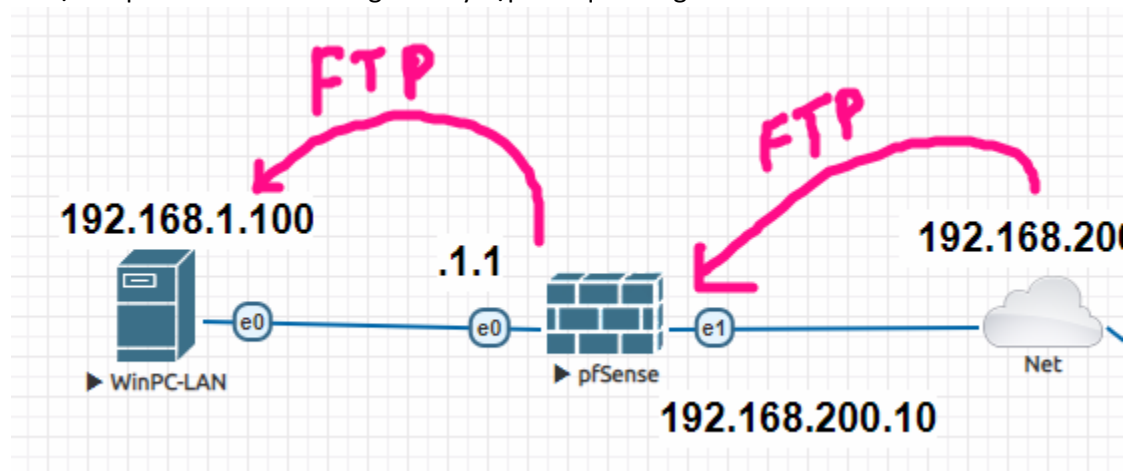
Rebooting
Page will automatically reload in 21 seconds

Package Installation


```
All repositories are up to date.  
Checking integrity... done (0 conflicting)  
The following 1 package(s) will be affected (of 0 checked):  
  
Installed packages to be UPGRADED:  
  pfSense-kernel-pfSense: 2.3 -> 2.3.4_1 [pfSense-core]  
  
Number of packages to be upgraded: 1  
[1/1] Upgrading pfSense-kernel-pfSense from 2.3 to 2.3.4_1...  
[1/1] Extracting pfSense-kernel-pfSense-2.3.4_1: ..... done  
==> Keeping a copy of current kernel in /boot/kernel.old  
Upgrade is complete. Rebooting in 10 seconds.  
>>> Locking package pfSense-kernel-pfSense... done.  
Success
```


9. Port forwarding


Ví dụ mở port 21 FTP cho từ ngoài truy cập vào qua cổng WAN






Ta vào Firewall > NAT > Add, sau đó điền như dưới để mở port 21


Interface WAN 
Choose which interface this rule applies to. In most cases "WAN" is specified.


Protocol TCP/UDP 
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source  Display Advanced


Destination Invert match. WAN address  Address.
Type Custom

Destination port range FTP  From port Custom FTP  To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be le

Redirect target IP 192.168.1.10  IP LAN
Enter the internal IP address of the server on which to map the ports.

Filter rule association Rule NAT FTP public 




Rule Information

- None
- Pass
- Rule NAT FTP public
- Create new associated filter rule 

Created 5/26/22 17:33:16 by admin@192.168.1.10

Sau đó ở bên Mục Firewall > Rules > WAN sẽ tự động tạo ra rule allow từ internet được truy cập vào FTP server.

Ta kích vào 2 rule block ở phía trên rồi disable nó đi, để chỉ còn 2 rule allow FTP

Description	Actions
Block private networks	 
Block bogon networks	

Reserved Networks

Block private networks and loopback addresses **BO³**
Blocks traffic from IP addresses that are reserved by RFC 4193 (fc00::/7) as well as loopback and private address space, too.

Block bogon networks **BO**
Blocks traffic from reserved IP addresses (both in the routing table, and so should not appear as though they are). The update from the routing table is shown below.

Ngoài ra có thể tự tạo 1 rule deny all ở cuối, kết quả như dưới:

Floating **WAN** LAN

Rules (Drag to Change Order)

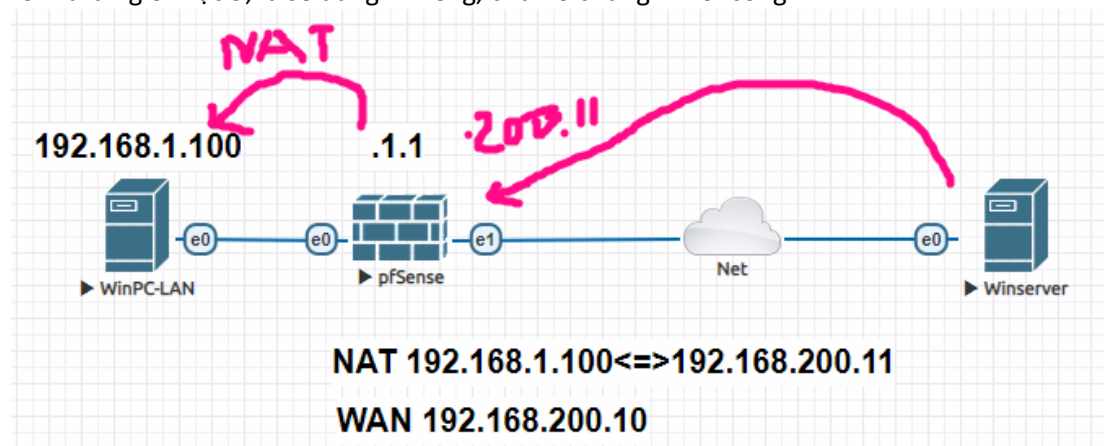
	States	Protocol	Source	Port	Destination	Port	Gateway	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	192.168.200.10	21 (FTP)	*
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 808 B	IPv4 *	*	*	*	*	*

CHECK LẠI:

Từ 1 máy bên ngoài mạng, ta dùng Filezilla để truy cập vào IP WAN, port 21, thấy connect thành công là ok

10. Static NAT public dịch vụ ra mạng

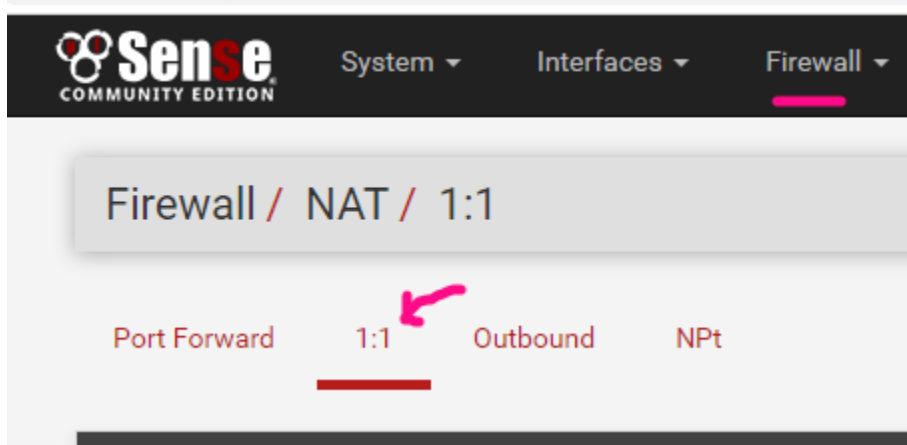
Mục đích: public dịch vụ ra mạng internet để ở ngoài có thể truy cập được, tuy nhiên khác với port-forwarding ở mục 9, là sẽ dùng IP riêng, chứ ko chung IP với cổng WAN.



https://hainguyenit.edubit.vn

Trong mô hình trên, máy PC Local sẽ chạy dịch vụ FTP và được Pfsense NAT ra thành IP 192.168.200.11 và listen ở cổng 21. Sau đó 1 máy từ ngoài WAN sẽ kết nối FTP vào qua IP NAT đó.

- Vào Firewall > NAT > Bấm tab 1:1 > bấm nút Add




- Điền như dưới và save lại


Interface	WAN	Choose which interface this rule applies to. In most cases "WAN" is specified.			
External subnet IP	192.168.200.11	Enter the external (usually on a WAN) subnet's starting address for the 1:1 mapping. The subnet mask from the internal address below will be applied to this IP address.			
Internal IP	<input type="checkbox"/> Not	Single host or alias	192.168.1.100	/	
	Invert the sense of the match.	Type	Address/mask		

- Vào Firewall > Rule > Chọn WAN, thêm 1 rule như dưới để allow TCP-21 từ ngoài vào:


https://hainguyenit.edubit.vn


Action 
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.



Interface 
Choose the interface from which packets must come to match this rule.



Address Family
Select the Internet Protocol version this rule applies to


Protocol 
Choose which IP protocol this rule should match.

Source Invert match.  /




Display Advanced

Destination Invert match.  

Destination port range  
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Options Log  Log packets that are handled by this rule

- Kết quả được rule:

Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
IPv4 TCP	*	*	192.168.1.100	21 (FTP)	*	none		allow FTP from outside	  

- Test lại: Trên server LAN cài Filezilla để làm FTP server (xem cách cài tại đây: bit.ly/hai-eve, mục số 6)
- > Trên client ngoài WAN, gõ telnet 192.168.200.11 21 để xem connect được chưa.
- > Trên firewall, Vào Status > System log để xem log truy cập đã được allow chưa

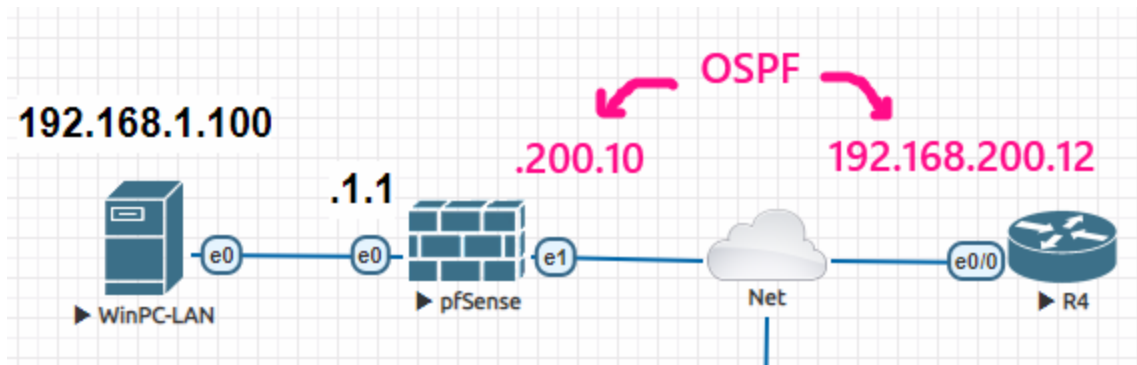
11. Cài gói và Cấu hình OSPF

- Download gói OSPF về

Vào System > Package Manager > Tab Available Packages > Gõ OSPF

Nhấn vào install Quagga OSPF để cài, chờ 1-3 phút cho cài xong

- Mô hình:



- Khai báo OSPF trên Pfsense:

Vào Service > Quagga OSPF > điền như dưới:

Services / Quagga OSPFd / Global Settings

Global Settings Interface Settings Raw Config Status

General Options

Master Password	12345 ← điền bất kì	Password to access the Zebra and OSPF management daemons. Required.
Logging	<input type="checkbox"/> If set to yes, Logs will be written via syslog.	
Log Adjacency Changes	<input type="checkbox"/> If set to yes, adjacency changes will be written via syslog.	
Router ID	192.168.200.10 ←	Specify the Router ID. RID is the highest logical (loopback) IP address configured on a router. For more information on router identifiers see wikipedia .
Area	0.0.0.0 ←	OSPFd area for this instance of OSPF. For more information on Areas see wikipedia .
Disable FIB updates (Routing table)	None (FIB updates enabled) (default) ▼	Disables the updating of the host routing table (turns into stub router).
Redistribute connected subnets	<input checked="" type="checkbox"/> Enables the redistribution of connected networks (Default no) ← Để quảng bá dải LAN cho router R4 biết	
Redistribute default route	<input type="checkbox"/> Enables the redistribution of a default route to this device (Default no)	

- Sang tab Interface Settings, chọn interface nào chạy OSPF rồi save lại:

Global Settings **Interface Settings** Raw Config Status

General Options

Interface	WAN ←	Enter the desired participating interface here.
Network Type	Broadcast ←	Select OSPF Network Type of the interface.
Metric		Metric (cost) for this OSPF interface (leave blank for default).
Area	0.0.0.0 ←	The area for this interface (leave blank for default).

- Khai báo trên Router R4

```
router ospf 1
int e0/0
ip address 192.168.200.12 255.255.255.0
ip ospf 1 area 0
```

- Check lại: **show ip ospf neighbor** trên Router

```
R4#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address        Interface
192.168.200.10  1     FULL/BDR       00:00:39   192.168.200.10 Ethernet0/0
R4#
```

show ip route trên router

```
O E2 192.168.1.0/24 [110/20] via 192.168.200.10, 00:15:04, Ethernet0/0
O E2 192.168.200.0/24 is variably subnetted, 3 subnets, 2 masks
C     192.168.200.0/24 is directly connected, Ethernet0/0
O     192.168.200.11/32 [110/20] via 192.168.200.10, 00:15:04, Ethernet0/0
L     192.168.200.12/32 is directly connected, Ethernet0/0
R4#
```

Để xem status OSPF trên Pfsense, vào các mục truy vấn như hình dưới:

Services / Quagga OSPF / Status

[Settings](#) [Interface Settings](#) [RAW Config](#) [Status](#)

Detailed OSPF status Information.

- [Quagga OSPF General](#)
- [Quagga OSPF Neighbors](#)
- [Quagga OSPF Database](#)
- [Quagga OSPF Router Database](#)
- [Quagga OSPF Routes](#)
- [Quagga Zebra Routes](#)
- [Quagga OSPF Interfaces](#)
- [Quagga OSPF CPU Usage](#)
- [Quagga OSPF Memory](#)
- [Quagga ospfd.conf](#)
- [Quagga zebra.conf](#)

12. Cấu hình VPN (còn tiếp)