

🔑 YÊU CẦU TRƯỚC KHI TRIỂN KHAI:

- Hai thiết bị pfSense** (vật lý hoặc ảo hóa), cài đặt giống nhau.
- Cấu hình **tối thiểu 3 interface** trên mỗi thiết bị:
 - WAN (kết nối internet)
 - DMZ
 - SOC
 - SYNC (đồng bộ CARP + XMLRPC)
- Địa chỉ IP riêng biệt** cho mỗi interface và **một IP ảo CARP** dùng chung cho cả 2 thiết bị.

🔗 CẤU HÌNH ĐỊA CHỈ IP & KẾT NỐI MẠNG

Trên pfSense Master:

Interface	IP thực	IP ảo CARP	Ghi chú
-----------	---------	------------	---------

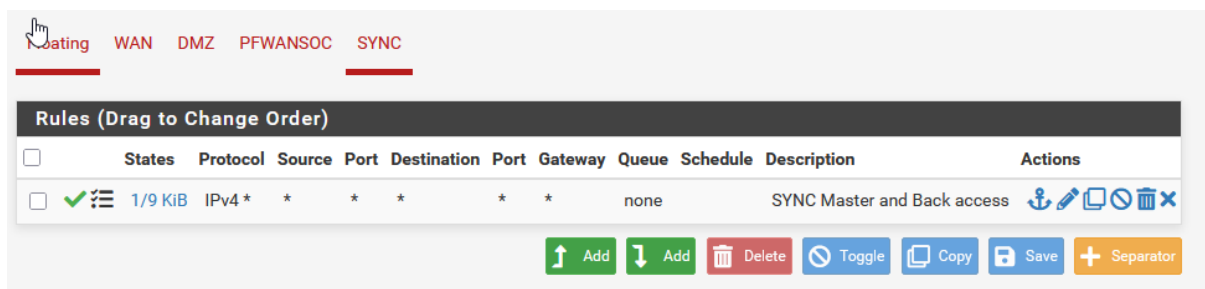
WAN	192.168.1.22/24	192.168.1.254/24	IP ảo public
DMZ	172.16.10.5/24	172.16.10.254/24	IP ảo cho DMZ
SOC	22.22.22.1/29	22.22.22.5/29	IP ảo cho SOC tới Pfsense-soc
SYNC	11.11.11.1/30	Không cần IP ảo	Chỉ dùng để đồng bộ

Trên pfSense Backup:

Interface	IP thực	IP ảo CARP	Ghi chú
WAN	192.0.2.21/24	192.168.1.254/24	IP ảo public
DMZ	172.16.10.6/24	172.16.10.254/24	IP ảo cho DMZ
SOC	22.22.22.3/29	22.22.22.5/29	IP ảo cho SOC tới Pfsense-soc
SYNC	10.0.0.2/24	Không cần IP ảo	Chỉ dùng để đồng bộ

Đảm bảo PF-MASTER và PF-BACK kết nối liên hệ với nhau, ping được

Trường hợp không thể ping được với nhau thì kiểm tra Rules trên interface SYNC



Cấu hình Gateway và Group Gateway giống nhau giữa 2 PF-MASTER và PF-BACK:

Đặc điểm chính trong WAN cần trỏ vào VIP WAN thì mới ra được internet khi có failover tự động.

Nếu có máy chủ DNS nội bộ thì nên cấu hình trỏ trực tiếp đến máy chủ DNS nội bộ đó

Bước 1: Thiết lập Virtual IPs trên PF-MASTER và PF-BACK

PF-MASTER:

Truy cập vào Firewall->Virtual IPs->Add

Thiết lập cho từng interfaces mạng trên PF-MASTER hiện có vào tạo VIP cho MASTER và BACK

Virtual IP này sẽ chịu trách nhiệm điều hướng chính giữa 2 pfsense với nhau. Ví dụ trên WAN thì gói tin sẽ được đưa ra ngoài internet qua VIP này.

Nên cần lưu ý xem xét cấu hình của route trên PF-MASTER để có cấu hình phù hợp

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface WAN

Address type Single address

Address(es) 192.168.1.254 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 1
Enter the VHID group that the machines will share.

Advertising frequency 1 0
Base Skew
 The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description PFWAN-VIP
A description may be entered here for administrative reference (not parsed).

Lưu ý:

- +Thứ tự của VHID Group phải giống nhau giữa 2 pfSense.
- +Virtual IP password đặt giống nhau trên từng VIP.
- +Để phân chia xem pfSense nào là master dựa vào CARP – Advertising Frequency

Trong CARP (Common Address Redundancy Protocol), mỗi node (Master/Backup) sẽ **gửi** “**CARP advertisements**” **định kỳ** để thông báo:

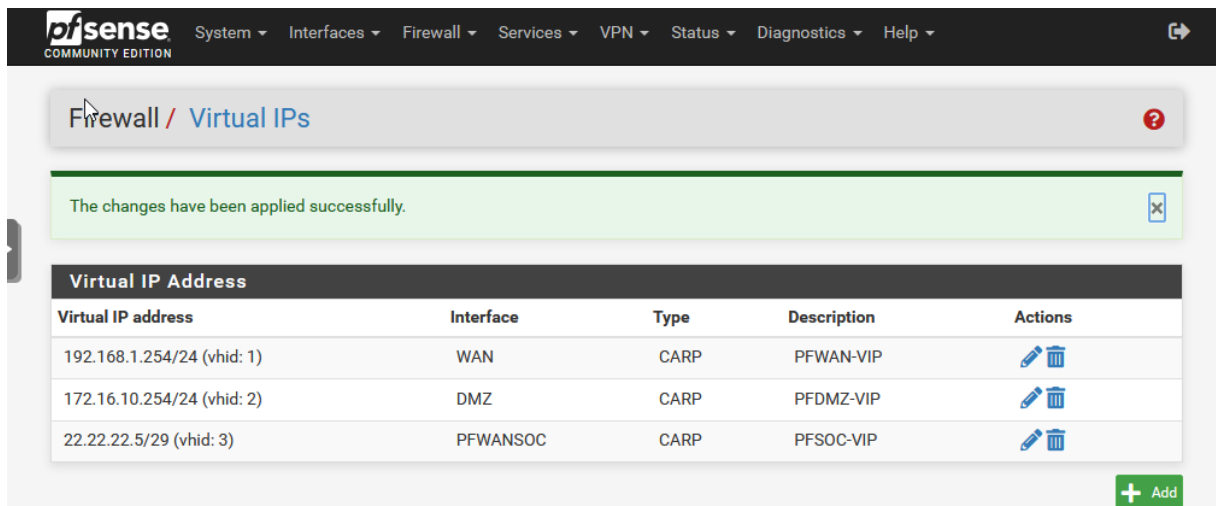
“Tôi đang ở đây, và tôi là Master!”

Tần suất gửi gói này = Base + Skew

Cách tính Advertising Frequency: CARP Advertisement Interval = (Base * 256 + Skew) / 100

- Base: Số giây cơ bản giữa các lần gửi (thường là 1 giây trên Master).
- Skew: Độ ưu tiên → càng **thấp** thì càng **ưu tiên** làm Master.

Thông thường thì trên PF-MASTER sẽ đặt Skew là 0 và PF-BACK sẽ đặt Skew là 100



Mở rộng:

Trong pfSense, hoàn toàn có thể **tạo nhiều Virtual IPs (VIPs) trên cùng một interface** – và đây là điều hoàn toàn bình thường, **thường được dùng khi triển khai CARP High Availability**.

Ví dụ thực tế:

Interface **WAN** với IP thật là 203.0.113.10. Muốn chạy nhiều dịch vụ (web, mail, VPN) qua các địa chỉ IP ảo riêng biệt, thì có thể tạo:

VIP Name	VIP Address	VHID	Interface	Ghi chú
VIP_Web	203.0.113.100 1		WAN	Web server
VIP_Mail	203.0.113.101 2		WAN	Mail server
VIP_VPN	203.0.113.102 3		WAN	VPN access

Bước 2: KÍCH HOẠT CARP & ĐỒNG BỘ

Trên PF-MASTER

Truy cập: System->High Availability

Cấu hình phần Configuration Synchronization Settings (XMLRPC Sync)

Configuration Synchronization Settings (XMLRPC Sync)	
Synchronize Config to IP	<input type="text" value="11.11.11.2"/> Enter the IP address of the firewall to which the selected configuration sections should be synchronized. XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly! Do not use the Synchronize Config to IP and password option on backup cluster members!
Remote System Username	<input type="text" value="admin"/> Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!
Remote System Password	<div> <input type="password" value="••••••••"/> <input type="password" value="••••••••"/> </div> Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!
Synchronize admin	<input checked="" type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Trong phần:

+ Synchroniza Config to IP: thì nhập IP của PF-BACK(11.11.11.2/29)

Khi đồng bộ thì dữ liệu sẽ được gửi hoặc liên hệ đến với IP của PF-BACK

+ Remote System Username: đây sẽ là tên tài khoản truy cập vào PF-BACK


+ Remote System Password: mật khẩu của tài khoản

+ Synchronize admin: lưu chọn có đồng bộ cả tài khoản mật khẩu của PF-MASTER tới PF-BACK

Select options to sync

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

☒ Toggle All

 Save


Cuối cùng là chọn hết hoặc chọn những phần cần đồng bộ với PF-BACK

➔ SAVE

[Trên PF-BACK](#)

Truy cập: System->High Availability

Cấu hình phần State Synchronization Settings(pfsync)

System / High Availability 

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface

SYNC

If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID

ba889782

Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP

11.11.11.1

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

- + Tích chọn Synchroniza states: sẽ nhận dữ liệu động bộ qua giao diện mạng SYNC
 - + Synchroniza Interface chọn giao diện mà động bộ nội bộ dữ 2 Pfsense hoặc nhiều Pfsense nếu mở rộng
 - + Filter Host ID: là một mã chuỗi định danh cho CARP mỗi CARP sẽ có chuỗi khác nhau vào không trùng với CARP khác
 - + pfsync Synchronize Peer IP: nhập IP của PF-MASTER
- ➔ SAVE