

**📌 YÊU CẦU TRƯỚC KHI TRIỂN KHAI:**

1. **Hai thiết bị pfSense** (vật lý hoặc ảo hóa), cài đặt giống nhau.
2. Cấu hình **tối thiểu 3 interface trên mỗi thiết bị**:
   * WAN (kết nối internet)
   * DMZ
   * SOC
   * SYNC (đồng bộ CARP + XMLRPC)
3. **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**:

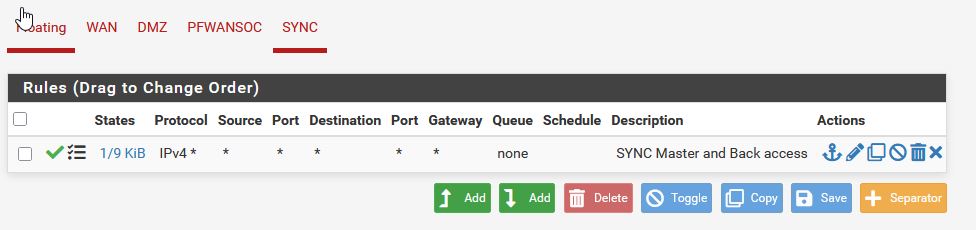
|  |  |  |  |
| --- | --- | --- | --- |
| **Interface** | **IP thực** | **IP ảo CARP** | **Ghi chú** |
| WAN | 192.168.1.22/24 | 192.168.1.254/24 | IP ảo public |
| DMZ | 172.16.10.5/24 | 172.16.10.254/24 | IP ảo cho DMZ |
| SOC | 22.22.22.1/29 | 22.22.22.5/29 | IP ảo cho SOC tới Pfsense-soc |
| SYNC | 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 |

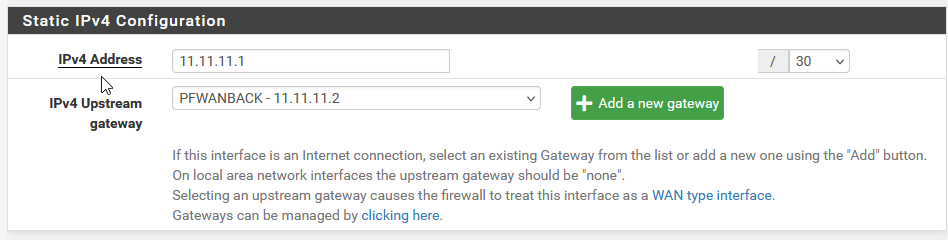
Đảm bảo PF-MASTER và PF-BACK kết nối liên hệ với nhau, ping được

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

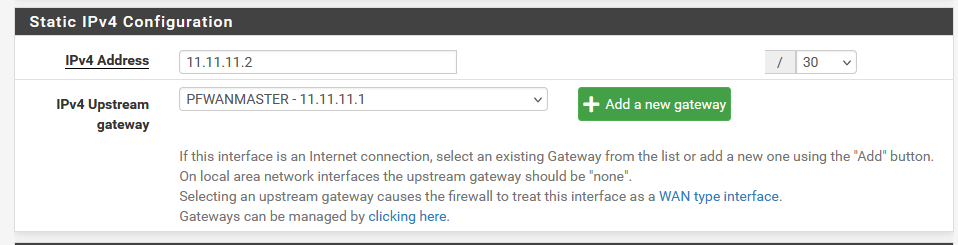


Giao diện SYNC đồng bộ giữa 2 pfsense:

PF-MASTER



PF-BACK

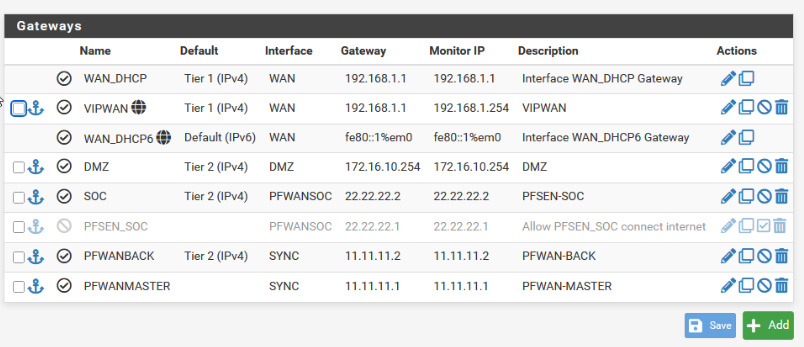


Cấu hình Gateway và Group Gateway giống nhau giữa 2 PF-MASTER và PF-BACK:

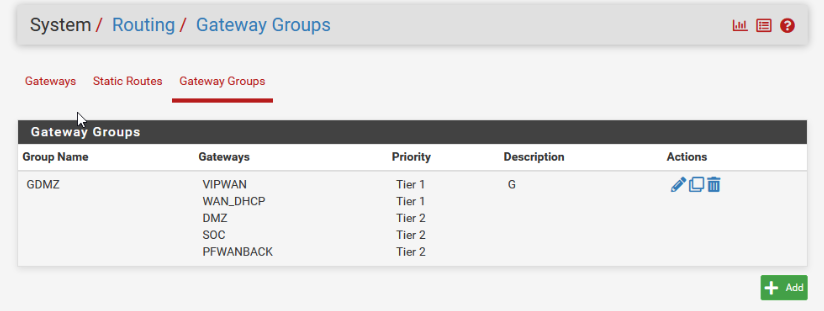
Đặc điểm chính trong WAN cần trỏ vào VIP WAN thì mới ra được internet khi có failover tự động.

Trên PF-MASTER

Gateway:



Gateway Group



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

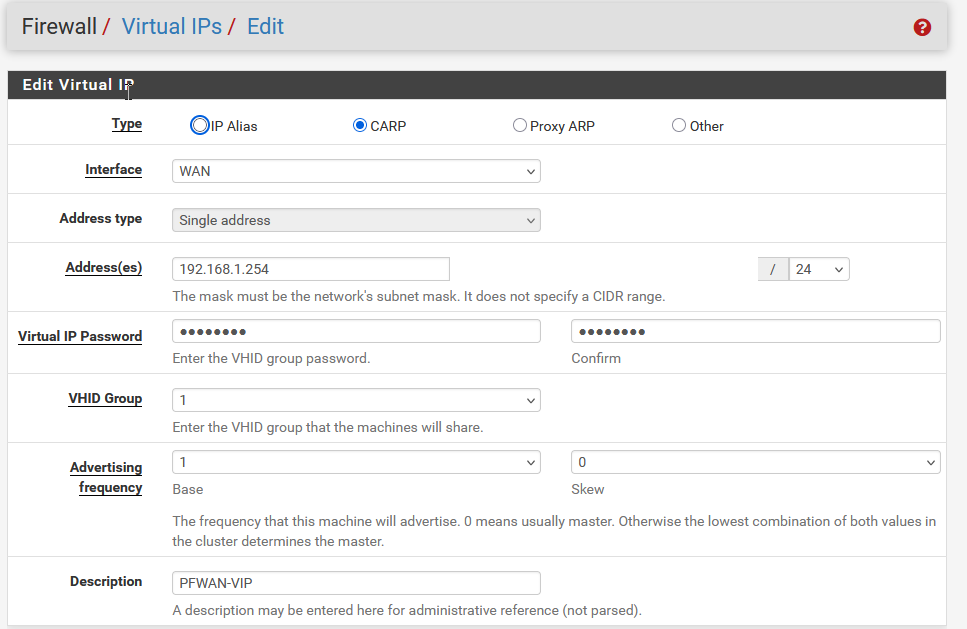
PF-MASTER:

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 tránh 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



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!”

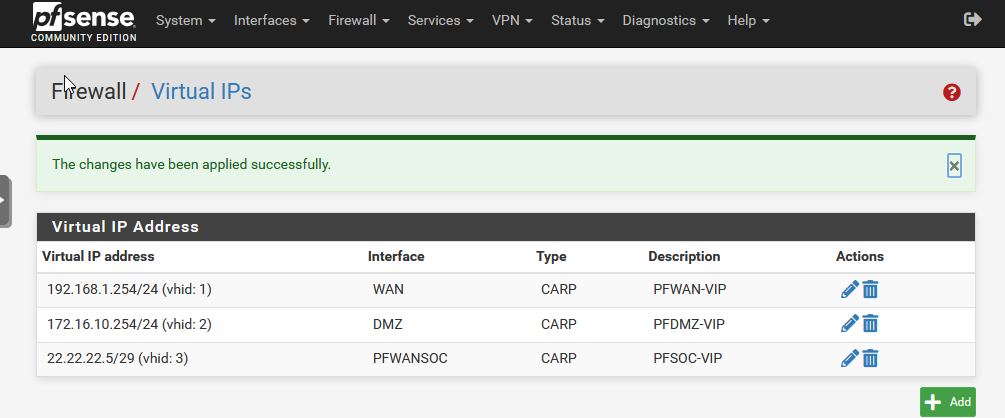
**Tần suất gửi gói này = Base + Skew**

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:

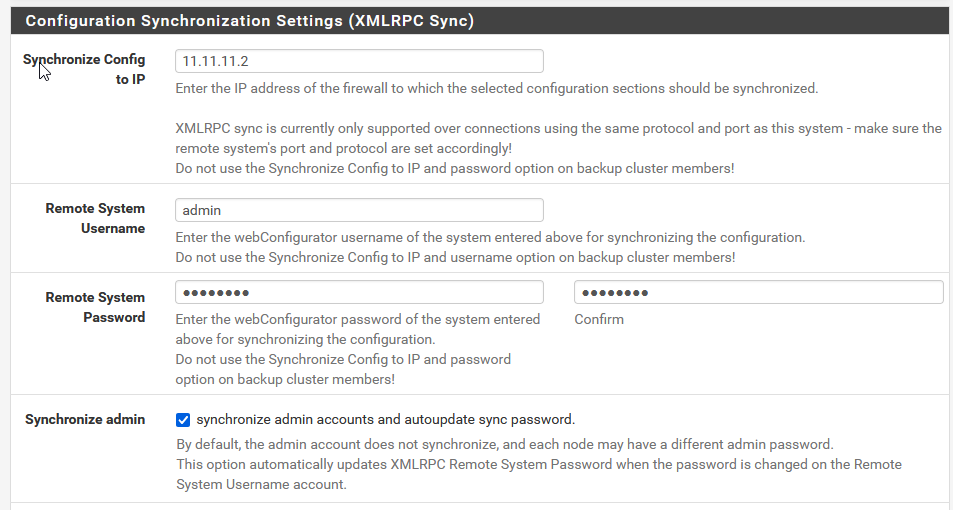
| **VIP Name** | **VIP Address** | **VHID** | **Interface** | **Ghi chú** |
| --- | --- | --- | --- | --- |
| VIP\_Web | 203.0.113.100 | 1 | WAN | Web server |
| VIP\_Mail | 203.0.113.101 | 2 | WAN | Mail server |
| VIP\_VPN | 203.0.113.102 | 3 | WAN | VPN access |

Bước 2: KÍCH HOẠT CARP & ĐỒNG BỘ

Trên PF-MASTER

Truy cập: System->High Availability

Cấu hình phần Configuration Synchronization Settings (XMLRPC Sync)



Trong phần:

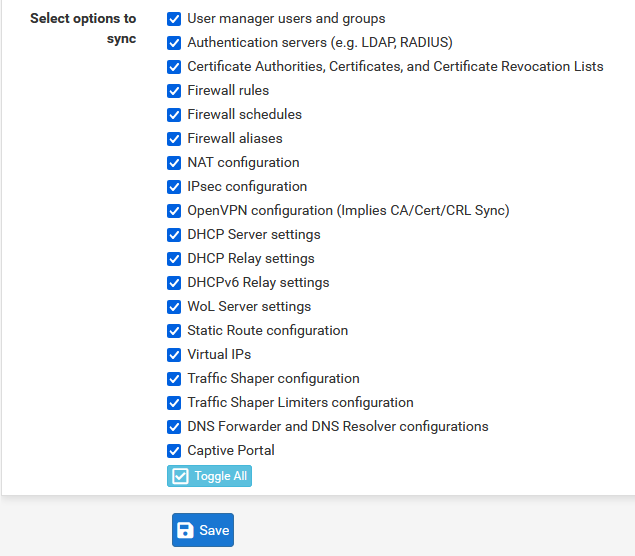
+ Synchroniza Config to IP: thì nhập IP của PF-BACK(11.11.11.2/29)

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



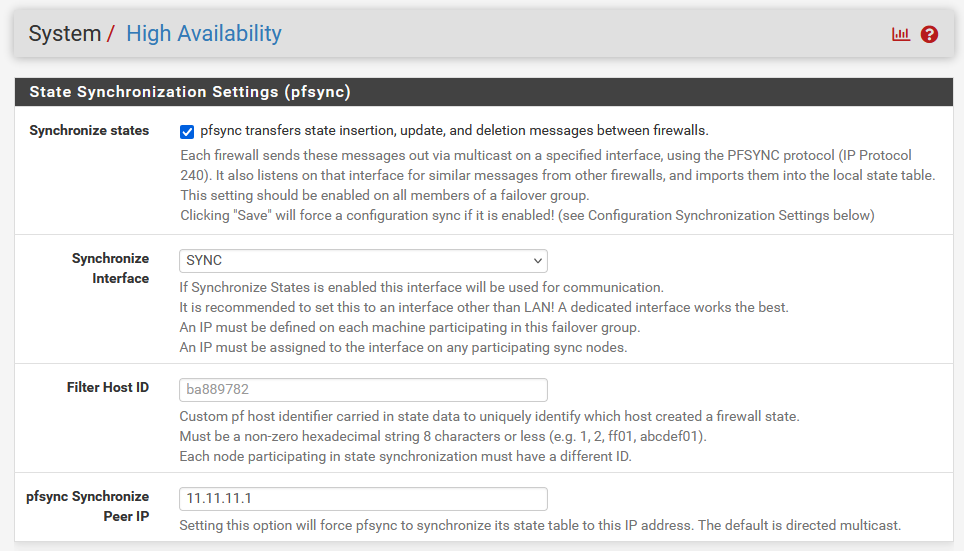
Cuối cùng là chọn hết hoặc chọn những phần cần đồng bộ với PF-BACK

* SAVE

Trên PF-BACK

Truy cập: System->High Availability

Cấu hình phần State Synchronization Settings(pfsync)



+ Tích chọn Synchroniza states: sẽ nhận dữ liệu động bọ qua giao diện mạng SYNC

+ Synchroniza Interface chọn giao diện mà động bộ nội bộ dữ 2 Pfsense hoặc nhiểu Pfsense nếu mở rọng

+ Filter Host ID: là một mã chuỗi định dạnh 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

## 📌 Tóm tắt ngắn gọn:

❌ **Gateway không đồng bộ qua XMLRPC Sync** → **phải tự tạo thủ công** trên cả 2 node (Master và Backup).

|  |  |
| --- | --- |
| Gateway (Static/Monitor) | ❌ Không (phải tạo thủ công) |

|  |  |
| --- | --- |
| Gateway Groups | ❌ Không (tạo tay trên cả 2) |

## 🧠 Lý do vì sao?

CARP và XMLRPC Sync chủ yếu được thiết kế để **đồng bộ cấu hình liên quan đến các dịch vụ mạng và firewall rules**, không phải mọi thứ trong hệ thống.  
**Gateway là một thành phần hệ thống cốt lõi (system routing), nên không được sync qua.**