
Triển Khai Load Balancing/Failover 2 WAN với Gateway Groups trên pfSense

Phần 1: Kiểm tra và Cấu hình Giao diện WAN (WAN Interfaces)

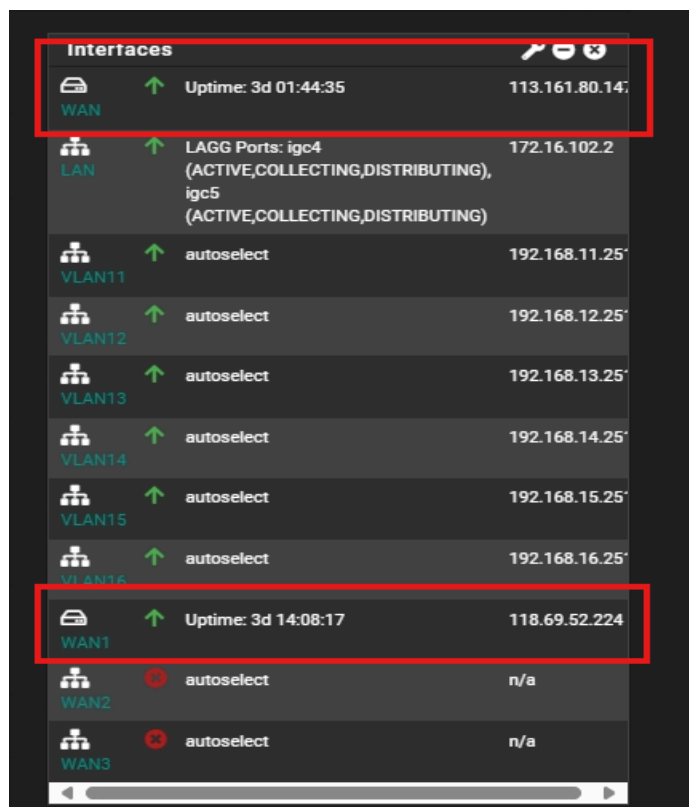
Trước tiên, cần đảm bảo cả hai đường truyền Internet đã được cấu hình và hoạt động đúng cách trên pfSense.

Bước 1.1: Xác định các Giao diện WAN

Hệ thống hạ tầng có hai giao diện WAN được thiết lập qua giao thức PPPoE:

- Giao diện WAN chính (WAN):**
 - Tên logic: WAN
 - Giao diện vật lý: pppoe0 (tương ứng với cổng igc0)
 - Nhà cung cấp: VNPT
- Giao diện WAN phụ (WAN1):**
 - Tên logic: WAN1 (được gán cho opt7)
 - Giao diện vật lý: pppoe1 (tương ứng với cổng igc1)
 - Nhà cung cấp: FPT

Lý do: Cần xác định chính xác các giao diện vật lý và logic của từng đường truyền WAN để có thể thêm chúng vào nhóm ở các bước tiếp theo.



Phần 2: Cấu hình Nhóm Gateway (Gateway Group)

Đây là bước cốt lõi để tạo ra cơ chế Load Balancing và Failover. Chúng ta sẽ tạo một nhóm chứa cả hai gateway của hai đường truyền WAN.

1. Truy cập **System > Routing > Gateway Groups**.
2. Nhấn **Add** để tạo một nhóm mới.
3. **Group Name**: Đặt tên cho nhóm, trong cấu hình này là VNPT_FPT.
4. **Gateway Priority (Cấu hình Tiers)**:
 - **Gateway WAN_PPPOE**: Chọn **Tier 1**.
 - **Gateway WAN1_PPPOE**: Cũng chọn **Tier 1**.
 - **Giải thích quan trọng**: Khi các gateway được đặt **cùng một Tier** (cùng cấp độ ưu tiên), pfSense sẽ thực hiện **Load Balancing** (phân tải) giữa chúng. Lưu lượng sẽ được phân phối trên cả hai đường truyền. Đồng thời, nếu một gateway trong cùng Tier bị down (mất kết nối), lưu lượng sẽ tự động được chuyển sang (các) gateway còn lại trong cùng Tier đó. Do đó, cấu hình này vừa là Load Balancing, vừa là Failover.
5. **Trigger Level**: Chọn Member Down. Tức là, pfSense sẽ coi một gateway là "lỗi" và ngừng gửi lưu lượng qua nó khi hệ thống giám sát phát hiện gateway đó bị mất kết nối (dựa trên packet loss hoặc latency cao).
6. **Description**: Thêm mô tả để dễ nhận biết, ví dụ WAN: VNPT | WAN1: FPT.
7. Nhấn **Save**.

Lý do: Gateway Group là một gateway "ảo" đại diện cho nhiều gateway thật. Bằng cách định tuyến lưu lượng qua nhóm này thay vì một gateway cụ thể, chúng ta cho phép pfSense tự động quản lý việc phân phối và chuyển đổi lưu lượng.

pfSense COMMUNITY EDITION

System / Routing / Gateway Groups / Edit

Edit Gateway Group Entry

Group Name VNPT_FPT

Gateway Priority

WAN_PPPOE	Tier 1	Interface Address	Interface WAN_PPPOE Gateway
WAN1_PPPOE	Tier 1	Interface Address	Interface WAN1_PPPOE Gateway

Gateway	Tier	Virtual IP	Description
---------	------	------------	-------------

Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.

Virtual IP The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.

Trigger Level Member Down
When to trigger exclusion of a member

Description WAN: VNPT | WAN1: FPT
A description may be entered here for administrative reference (not parsed).

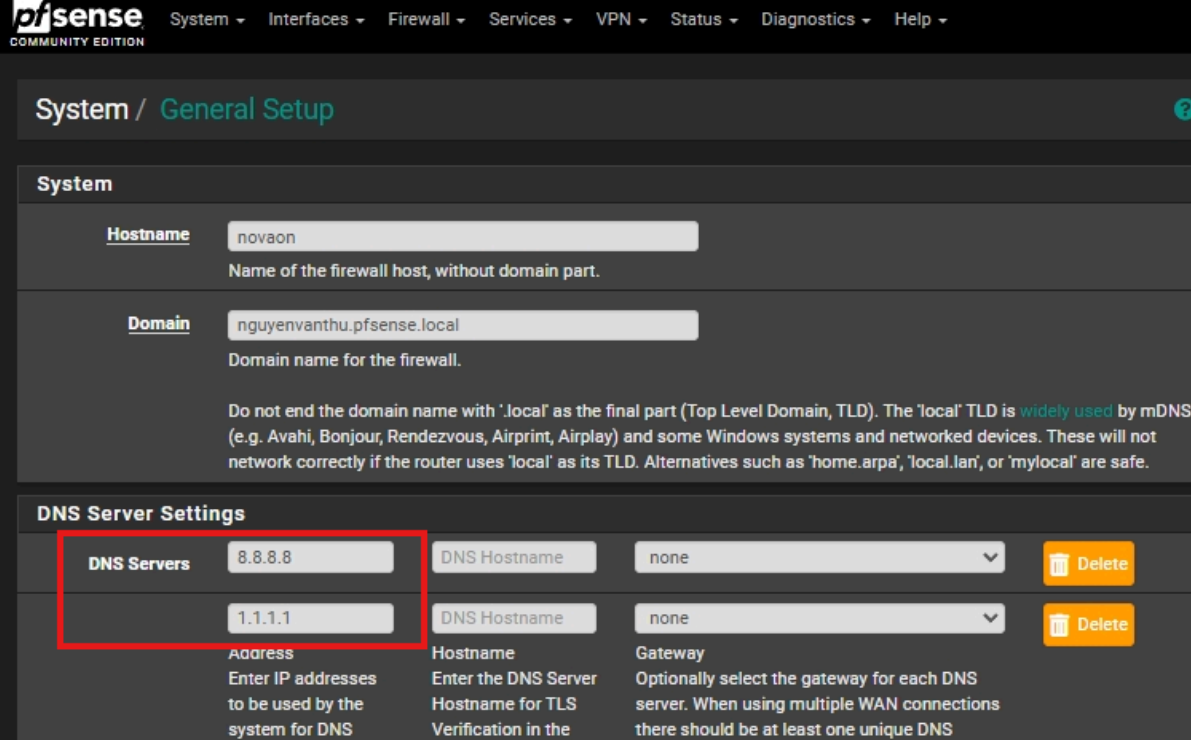
Save

Phần 3: Cấu hình DNS để hoạt động với Multi-WAN

Để đảm bảo việc phân giải tên miền không bị gián đoạn khi một đường WAN lỗi, cấu hình DNS cần được thiết lập đúng cách.

1. Truy cập **System > General Setup**.
2. **DNS Servers:** Đã cấu hình các máy chủ DNS công cộng là 8.8.8.8 và 1.1.1.1.
3. **DNS Server Gateway:** Đảm bảo rằng cột Gateway cho mỗi DNS server được đặt là none.

Lý do: Điều này cho phép pfSense truy vấn DNS qua bất kỳ gateway nào đang hoạt động. Nếu một WAN bị lỗi, các truy vấn DNS vẫn có thể đi qua WAN còn lại, tránh tình trạng "Internet down" chỉ vì không phân giải được tên miền.



The screenshot shows the pfSense web interface, specifically the 'System / General Setup' page. The 'System' section includes fields for 'Hostname' (novaon) and 'Domain' (nguyenvanthu.pfsense.local). Below this is the 'DNS Server Settings' section, which contains a table of DNS servers. The table has columns for 'DNS Servers', 'DNS Hostname', and 'Gateway'. Two entries are listed: 8.8.8.8 and 1.1.1.1, both with 'none' as the gateway. A red box highlights the 'DNS Servers' column and the two entries. Below the table, there are instructions for each column: 'Address' (Enter IP addresses to be used by the system for DNS), 'Hostname' (Enter the DNS Server Hostname for TLS Verification in the), and 'Gateway' (Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS).

DNS Servers	DNS Hostname	Gateway
8.8.8.8	none	none
1.1.1.1	none	none

Address
Enter IP addresses to be used by the system for DNS

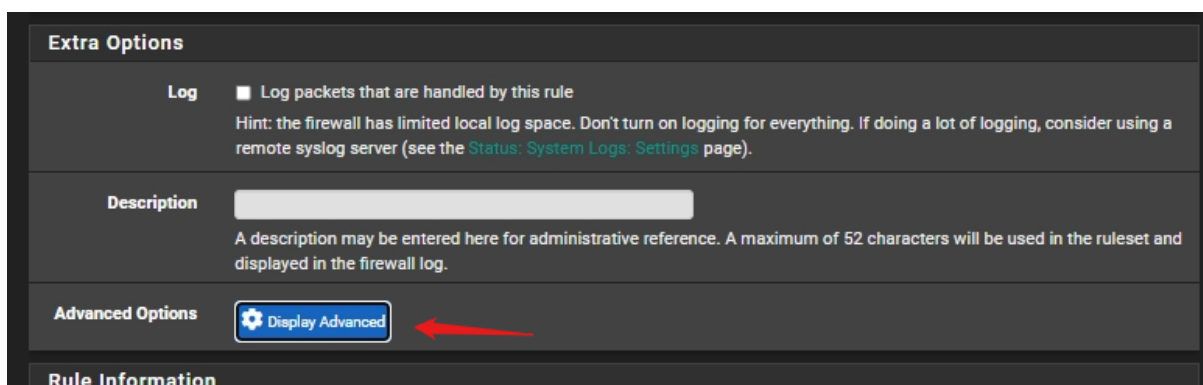
Hostname
Enter the DNS Server Hostname for TLS Verification in the

Gateway
Optionally select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS

Phần 4: Áp dụng Gateway Group vào Firewall Rules

Sau khi tạo Gateway Group, chúng ta cần chỉ cho tường lửa biết phải sử dụng nó. Ta sẽ sửa đổi quy tắc cho phép lưu lượng từ mạng LAN ra Internet.

1. Truy cập **Firewall > Rules > LAN** (và các giao diện VLAN khác như OPT1, OPT2, v.v.).
2. Tìm quy tắc cho phép lưu lượng ra ngoài.
3. Mở quy tắc đó lên để chỉnh sửa.
4. Kéo xuống dưới cùng và nhấn vào nút **Display Advanced**.



Extra Options

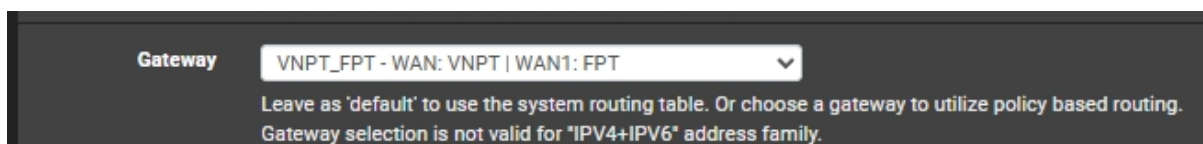
Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

5. Trong mục **Gateway**, chọn Gateway Group đã tạo ở Phần 2 (VNPT_FPT).

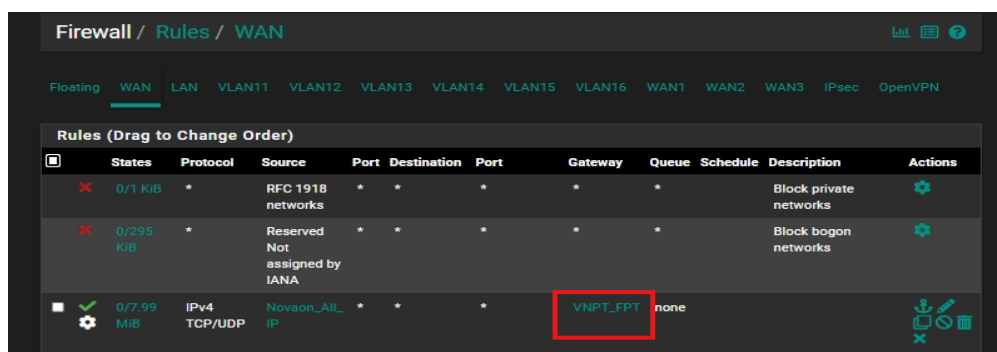


Gateway

Leave as 'default' to use the system routing table. Or choose a gateway to utilize policy based routing.
Gateway selection is not valid for 'IPv4+IPv6' address family.

6. Nhấn **Save** và **Apply Changes**.
7. Lặp lại thao tác này cho tất cả các quy tắc "pass" ra ngoài Internet của các giao diện mạng nội bộ khác (VLAN11, VLAN12, v.v.).

Lý do: Đây là bước quyết định để 'kích hoạt' việc phân tải. Bất kỳ lưu lượng nào khớp với quy tắc này sẽ không đi ra một WAN cụ thể mà sẽ được chuyển đến Gateway Group để pfSense xử lý việc phân tải và dự phòng.

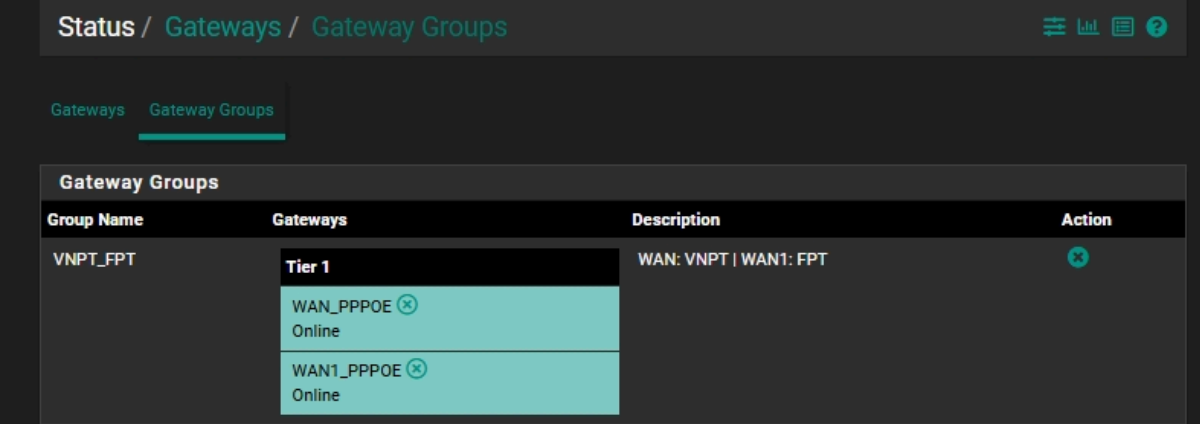


Firewall / Rules / WAN											
Floating WAN LAN VLAN11 VLAN12 VLAN13 VLAN14 VLAN15 VLAN16 WAN1 WAN2 WAN3 IPsec OpenVPN											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/1 KiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
<input checked="" type="checkbox"/>	0/295 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input checked="" type="checkbox"/>	0/7.99 MiB	IPv4 TCP/UDP	Novacon_Ail_IP	*	*	*	VNPT_FPT	none			




Phần 5: Kiểm tra và Giám sát

Sau khi hoàn tất cấu hình, việc kiểm tra trạng thái hoạt động là rất quan trọng.

1. Truy cập **Status > Gateways** hoặc **Status > Gateway Groups**.
2. Có thể thấy trạng thái của từng gateway (Online/Offline) và trạng thái của cả nhóm. Cả hai gateway trong nhóm VNPT_FPT phải hiển thị trạng thái "Online".
3. **Kiểm tra thực tế:**
 - Có thể kiểm tra bằng cách thử rút cáp mạng của một trong hai đường WAN.
 - Quan sát trong **Status > Gateways**, sẽ thấy gateway tương ứng chuyển sang trạng thái "Offline".
 - Kiểm tra xem các máy tính trong mạng nội bộ có còn truy cập được Internet qua đường truyền còn lại hay không. Kết nối phải được duy trì mà không bị gián đoạn.



The screenshot shows a web interface for monitoring network status. The breadcrumb navigation at the top is 'Status / Gateways / Gateway Groups'. Below this, there are two tabs: 'Gateways' and 'Gateway Groups', with 'Gateway Groups' being the active tab. The main content area displays a table for 'Gateway Groups'. The table has four columns: 'Group Name', 'Gateways', 'Description', and 'Action'. The first row shows a group named 'VNPT_FPT'. Under the 'Gateways' column for this group, there is a sub-header 'Tier 1' followed by two entries: 'WAN_PPPOE' and 'WAN1_PPPOE', both marked as 'Online' with a green checkmark icon. The 'Description' column for this group shows 'WAN: VNPT | WAN1: FPT'. The 'Action' column contains a green checkmark icon.

Gateway Groups			
Group Name	Gateways	Description	Action
VNPT_FPT	Tier 1	WAN: VNPT WAN1: FPT	
	WAN_PPPOE 		
	Online		
	WAN1_PPPOE 		
	Online		