□ Lab 5: Cấu hình DNS Resolver & Forwarder

🎯 Mục tiêu

- Hiểu rõ 2 chế độ xử lý DNS trong pfSense: **Resolver** và **Forwarder**.
- Cấu hình DNS nội bộ.
- Ghi log truy vấn DNS để giám sát hoặc lọc.
- Tùy chọn: Chặn DNS bên ngoài, ép dùng DNS nội bộ (pfSense).

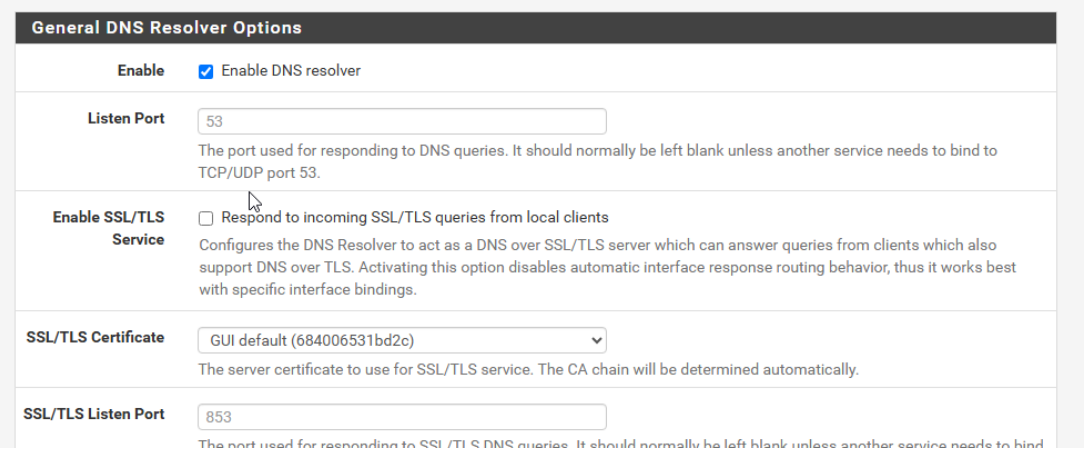
📋 Tổng quan DNS trong pfSense

Chế độ	Mô tả
DNS Resolver *(Unbound)*	Truy vấn DNS từ gốc (recursive). Bảo mật, không cần forward. Mặc định bật.
DNS Forwarder *(dnsmasq)*	Gửi truy vấn đến DNS bên ngoài như Google (8.8.8.8), Cloudflare...

🔧 Bước 1: Kiểm tra và bật DNS Resolver (mặc định)

1. Truy cập GUI pfSense → `https://192.168.20.1`
2. Vào **Services → DNS Resolver**
3. Đảm bảo:
   - ✅ **Enable DNS Resolver**: bật
   - ✅ **Enable DNSSEC Support**: bật (nếu muốn bảo mật truy vấn)
   - ✅ **DHCP Registration**: để tự thêm hostname các máy từ DHCP
   - ✅ **Static DHCP Registration**: nếu dùng Static Lease
4. **Save & Apply**

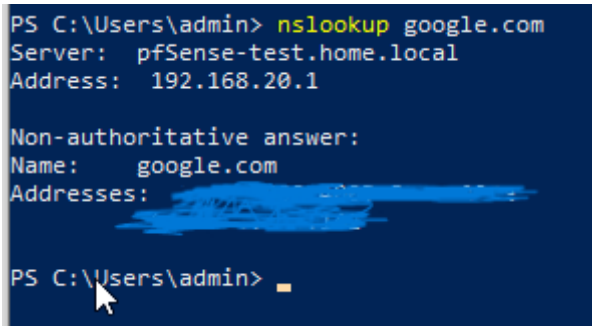
📌 Resolver sẽ tự phân giải DNS từ root, không cần forward ra ngoài.



💻 Bước 3: Đảm bảo client sử dụng pfSense làm DNS

1. Máy client được cấp DNS là `192.168.20.1` (qua DHCP)
2. Kiểm tra:

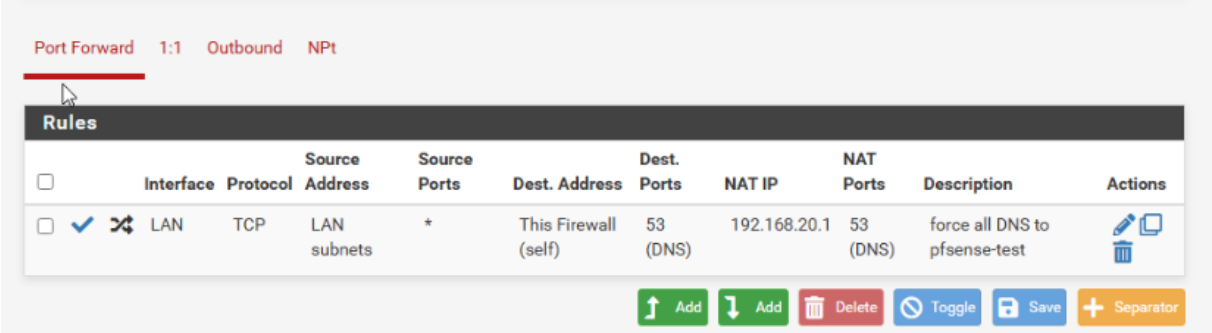
nslookup google.com



🔒 Bước 4: Ép buộc tất cả client dùng DNS của pfSense

1. Vào **Firewall → NAT → Port Forward**
2. Add rule trên **LAN interface**:
   - **Source**: LAN net
   - **Destination port**: 53 (DNS)
   - **Redirect target IP**: `127.0.0.1` (hoặc `192.168.10.1`)
   - **Redirect target port**: 53
   - ✅ **NAT Reflection**: Disable
   - **Description**: `Force all DNS to pfSense`
3. Save & Apply

👉 Tất cả DNS từ client sẽ bị ép qua pfSense, kể cả nếu họ cố dùng 8.8.8.8.



🧾 Bước 5: Ghi log truy vấn DNS

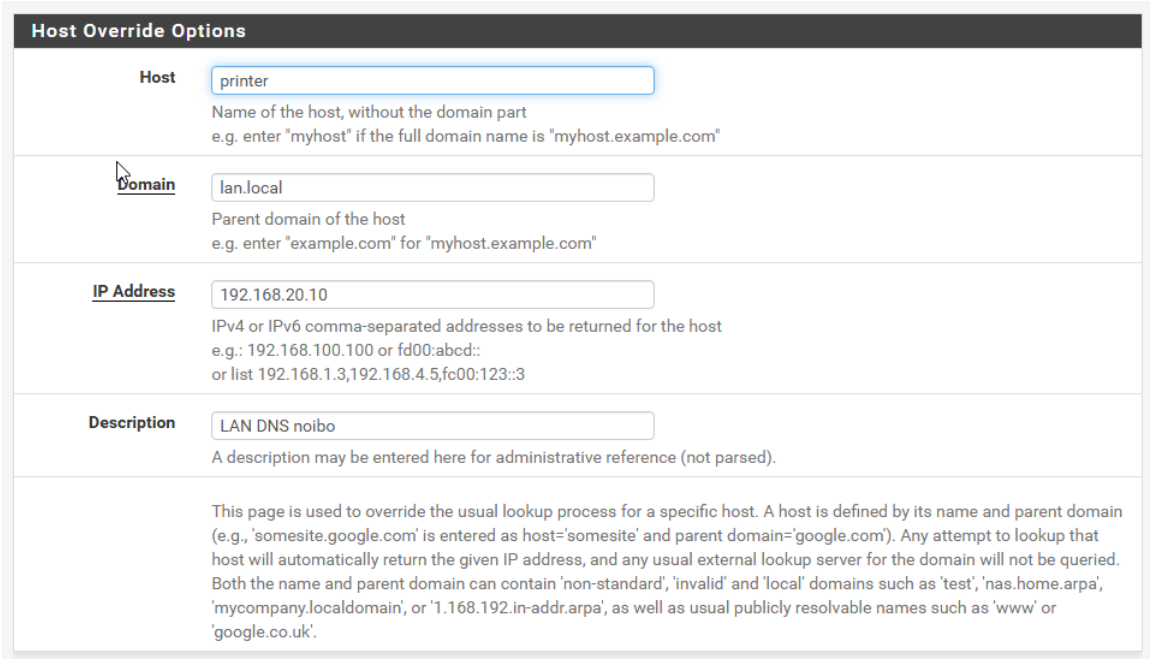
1. Vào **Services → DNS Resolver**
2. ✅ Tick **Enable Query Logging**
3. Apply Changes

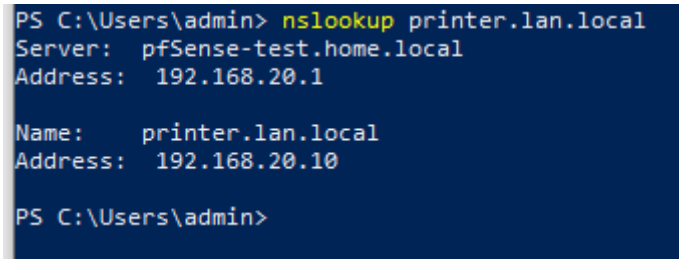
🔍 Xem log tại:
Status → System Logs → Resolver

Bạn có thể thấy từng domain được truy vấn, theo thời gian thực.

□ Bước 6: Cấu hình DNS nội bộ (hostname nội bộ tùy chỉnh)

1. Vào **Services → DNS Resolver → Host Overrides**
2. Bấm **Add**
   - **Host**: `printer`
   - **Domain**: `local.lan`
   - **IP address**: `192.168.20.10`
3. Client gõ `printer.local.lan` → sẽ được trả về IP nội bộ.





☑ Kết quả đạt được

- Đã bật Resolver hoặc Forwarder, DNS client đi qua pfSense.
- Log truy vấn DNS được ghi lại → hỗ trợ giám sát, lọc.
- Tùy chọn ép buộc mọi DNS đi qua pfSense để tăng kiểm soát.