

# ❑ 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
<b>DNS Resolver</b> (Unbound)	Truy vấn DNS từ gốc (recursive). Bảo mật, không cần forward. Mặc định bật.
<b>DNS Forwarder</b> (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.

General DNS Resolver Options

Enable

☒ Enable DNS resolver

Listen Port

The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service

☐ Respond to incoming SSL/TLS queries from local clients

Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate

GUI default (684006531bd2c)

▼

The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port

The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind

## 📁 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

```
PS C:\Users\admin> nslookup google.com
Server:  pfSense-test.home.local
Address:  192.168.20.1

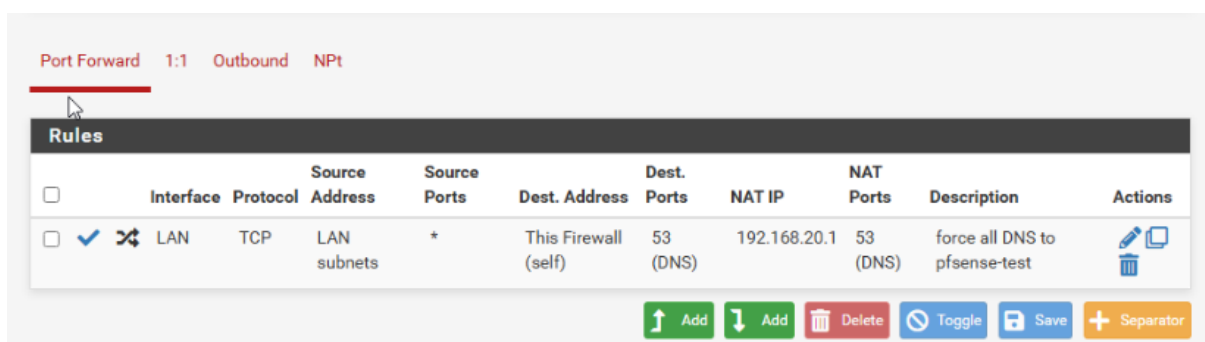
Non-authoritative answer:
Name:     google.com
Addresses: [REDACTED]

PS C:\Users\admin>
```

## 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. ☒ **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:** lan.local
  - **IP address:** 192.168.20.10
3. Client gõ `printer.lan.local` → sẽ được trả về IP nội bộ.

**Host Override Options**

**Host**   
Name of the host, without the domain part  
e.g. enter "myhost" if the full domain name is "myhost.example.com"

**Domain**   
Parent domain of the host  
e.g. enter "example.com" for "myhost.example.com"

**IP Address**   
IPv4 or IPv6 comma-separated addresses to be returned for the host  
e.g.: 192.168.100.100 or fd00:abcd::  
or list 192.168.1.3,192.168.4.5,fc00:123::3

**Description**   
A description may be entered here for administrative reference (not parsed).

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.

```
PS C:\Users\admin> nslookup printer.lan.local
Server:  pfSense-test.home.local
Address:  192.168.20.1

Name:     printer.lan.local
Address:  192.168.20.10

PS C:\Users\admin>
```

## ✓ 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.