



SERVIÇO DE DNS (RESOLVER/FORWARDER) - PFSENSE

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

Código: ITGINF 0019/26 | **Classificação:** RESTRITO

Responsável: João Pedro Toledo Gonçalves | **Data:** 26/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
26/01/2026	1.0	Criação Inicial	João Pedro Toledo Gonçalves

2. OBJETIVO

Garantir a resolução de nomes (DNS) segura e rápida para a rede local, com capacidade de sobrescrever nomes específicos (Host Overrides) para serviços internos.

3. PRÉ-REQUISITOS

- ☐ pfSense com acesso à internet.
- ☐ DNS Upstream definidos (ex: Cloudflare 1.1.1.1, Google 8.8.8.8) se usar Forwarding.

4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: DNS Resolver (Unbound)

O Resolver é o método padrão e mais seguro (DNSSEC).

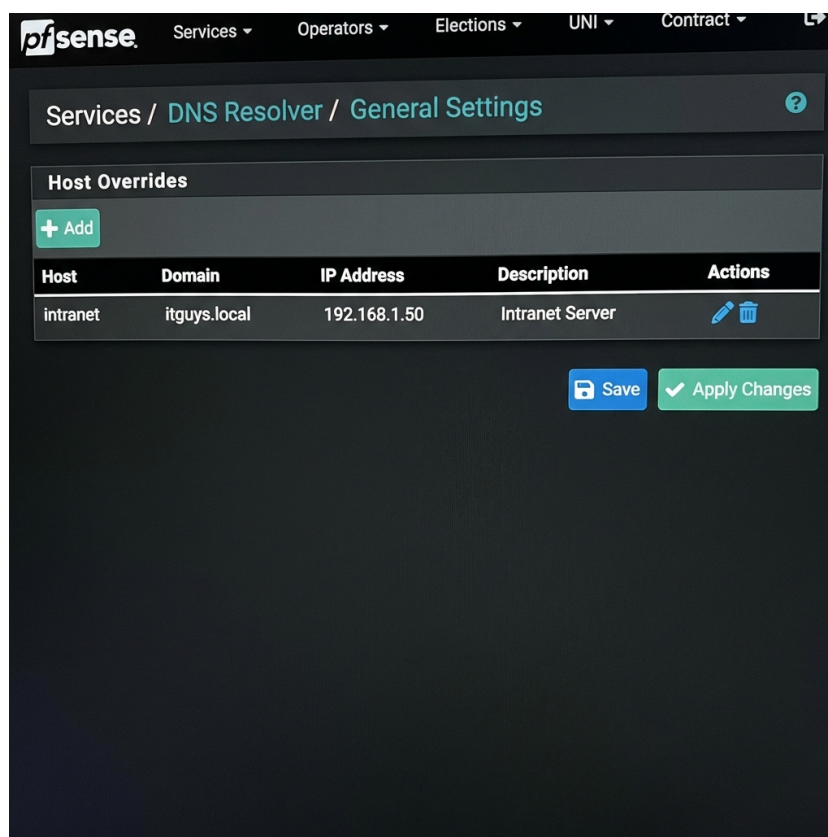
- ☒ Acesse `Services > DNS Resolver > General Settings`.
- ☒ Marque **Enable DNS Resolver**.
- ☒ **Network Interfaces:** Selecione `All` (ou apenas as interfaces LAN/VLANs onde o serviço deve escutar).
- ☒ **Outgoing Network Interfaces:** Selecione `WAN` (Por onde a consulta sai).
- ☒ **DNSSEC:** Marque **Enable DNSSEC Support** para proteção contra spoofing.
- ☒ **DNS Query Forwarding:**
 - **Desmarcado:** O pfSense resolve direto com os Root Servers (Mais privado, pode ser mais lento no início).
 - **Marcado (Enable Forwarding Mode):** O pfSense repassa para os DNS definidos em `System > General Setup` (Mais rápido se os DNS do ISP/Google forem bons).
 - **Recomendação:** Habilite se usar MultiWAN.

7. [x] Clique em **Save** e **Apply Changes**.

Etapa 2: Host Overrides (DNS Split)

Use para fazer com que `intranet.meudominio.com` aponte para um IP local (`192.168.1.x`) quando acessado de dentro da empresa.

1. [x] Role até o final da página **DNS Resolver**.
2. [x] Em **Host Overrides**, clique em **Add**.
3. [x] Preencha:
 - **Host:** `intranet`
 - **Domain:** `itguys.local`
 - **IP Address:** `192.168.1.50`
 - **Description:** Intranet Server
4. [x] Salve.



Etapa 3: Integração com Active Directory (Domain Override)

Se você tem um AD (`itguys.local`) mas quer que o pfSense seja o DNS principal dos clientes:

1. [x] Acesse `Services > DNS Resolver`.
2. [x] Role até **Domain Overrides**.
3. [x] Clique em **Add**.
 - **Domain:** `itguys.local`
 - **IP Address:** `192.168.1.10` (IP do Domain Controller).
4. [x] Salve.
 - > **Explicação:** O pfSense enviará qualquer consulta sobre `\*.itguys.local` para o AD, e resolverá o resto da internet sozinho.

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: DNS muito lento

- **Causa:** Root servers distantes ou problemas de rota.
- **Solução:** Ative o **DNS Query Forwarding** e use `1.1.1.1` e `8.8.8.8` em `System > General Setup`.

Problema 2: Não resolve nomes internos do AD

- **Causa:** Domain Override configurado errado ou Firewall bloqueando a porta 53 TCP/UDP entre pfSense e AD.
- **Solução:** Libere a porta 53 na regra de firewall da LAN/VLAN onde o AD está.

Problema 3: DNS Rebind Attack

- **Sintoma:** O pfSense bloqueia respostas que apontam para IPs privados (RFC1918).
- **Solução:** Se precisar disso (ex: Plex, serviços locais), adicione o domínio em `System > Advanced > Admin Access > DNS Rebind Check` ou use as opções customizadas (Advanced Settings) do Unbound: `private-domain: "meudominio.local"`.

6. DADOS TÉCNICOS

Campo	Valor	Descrição
Porta	53 (TCP/UDP)	Porta Padrão
DNSSEC	Ativo	Segurança Padrão
Service	Unbound	Resolver

7. VALIDAÇÃO FINAL (DEFINIÇÃO DE PRONTO)

- ☐ Clientes navegam na internet?
- ☐ Ping para `intranet.itguys.local` resolve o IP interno?
- ☐ `nslookup google.com` retorna resposta rápida?