



SERVIÇO DE DNS (RESOLVER/FORWARDER) - PFSENSE

Guia Oficial iT Guys

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

Responsável: João Pedro Toledo Gonçalves | **Data:** 25/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
25/01/2026	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).

1. Acesse `Services > DNS Resolver > General Settings`.
2. Marque **Enable DNS Resolver**.
3. **Network Interfaces:** Selecione `All` (ou apenas as interfaces LAN/VLANs onde o serviço deve escutar).
4. **Outgoing Network Interfaces:** Selecione `WAN` (Por onde a consulta sai).
5. **DNSSEC:** Marque **Enable DNSSEC Support** para proteção contra spoofing.
6. **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.

The screenshot shows the pfSense web administration interface. The top navigation bar includes 'Servers', 'Overview', 'Services', 'DNS', 'Report', 'Administration', and 'Help'. The breadcrumb trail is 'Services / DNS Resolver / General Settings'. The 'General Settings' section contains the following options:

- Enable DNS Resolver:** A checkbox labeled 'Enable DNS Resolver' is checked. Below it, a note says 'Enable DNS Resolver for your arxasss network, adminahates.'
- Network Interfaces:** A dropdown menu is set to 'All'. Below it, a note says 'Select the interfaces to ssta: and rall off oro-eined name cnd riors in ilakistert policy, network interfaces /net: network lntenark interfaces vible, network interfaces, siternet, and ro-enxrce sitanes sets.'
- Outgoing Network Interfaces:** A dropdown menu is set to 'WAN'. Below it, a note says 'Select the Network Interfaces lo WAN show its outgoing Network Interfaces for interfaces.'
- DNSSEC:** A checkbox labeled 'Enable DNSSEC Support' is checked. Below it, a note says 'Enable DNSSEC Support to be the cawar:rd IP /oan:mice for DNSSEC.'
- Python Module:** A checkbox labeled 'Enable Python Module' is unchecked. Below it, a note says 'Python Module provides use the DNSSEC using nifeatnon module's non edolt, you can use statutive configuration for no python module.'

At the bottom right of the settings area are 'Save' and 'Cancel' buttons. The footer of the interface reads 'pfSense is web administration - All rights reserved | ttestarner, Oct 15, 2021 at 12:39 AM'.

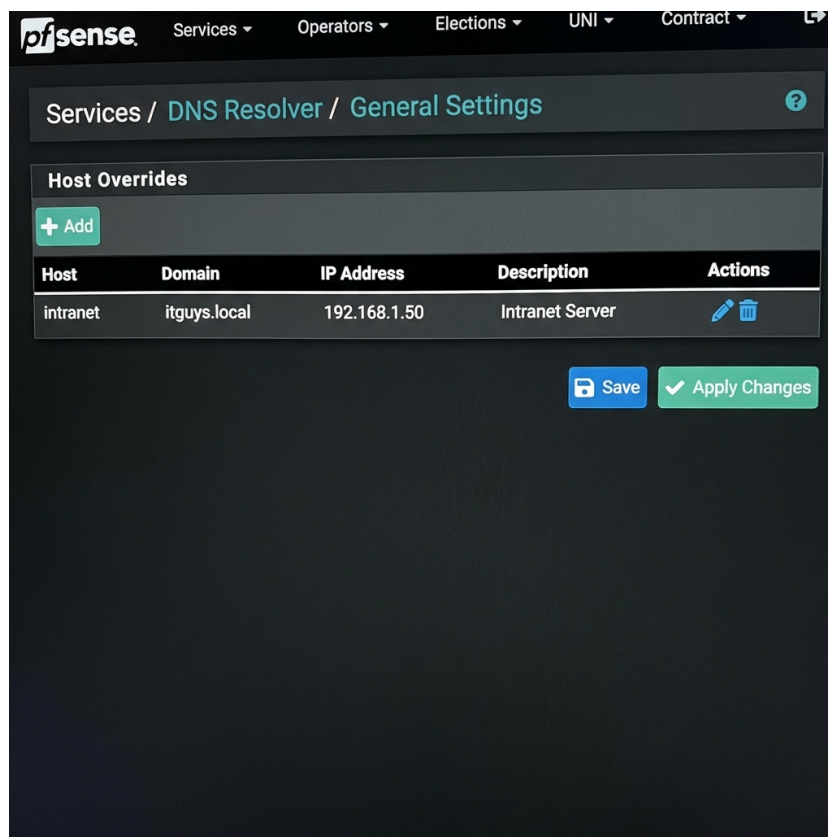
7. Clique em **Save** e **Apply Changes**.

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

4. 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. Acesse `Services > DNS Resolver`.
2. Role até **Domain Overrides**.
3. Clique em **Add**.
 - * **Domain:** `itguys.local`
 - * **IP Address:** `192.168.1.10` (IP do Domain Controller).
4. 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?