



FIREWALL RULES E NAT - PFSENSE

Guia Oficial iT Guys

Código: ITGINF 0018/26 | **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

Definir as regras de permissão de tráfego (Firewall) e redirecionamento de portas (NAT) para garantir a segurança e funcionalidade dos serviços publicados.

3. PRÉ-REQUISITOS

- [] Definição precisa das portas de origem e destino (ex: TCP 3389).
- [] IP interno do servidor destino fixado (Static Mapping).

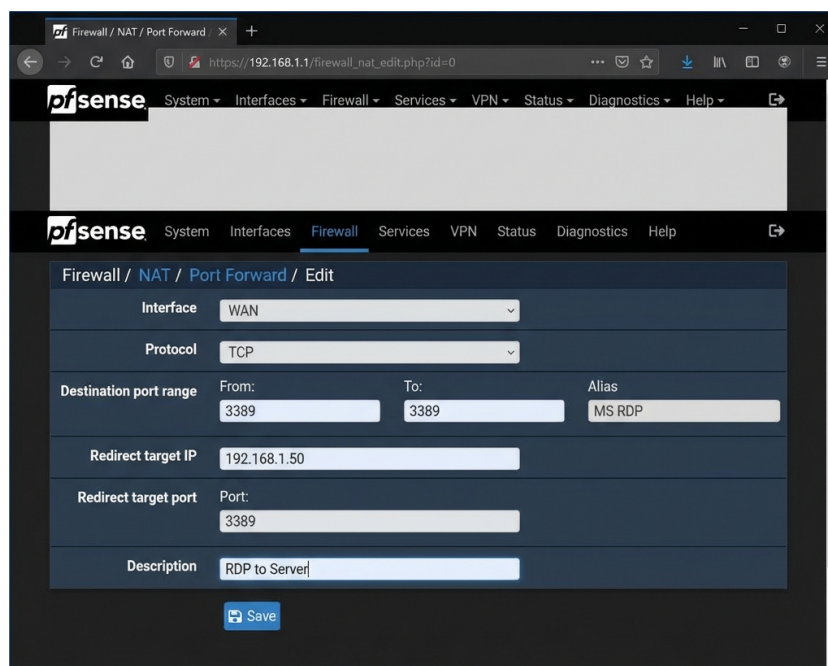
4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: Port Forward (Redirecionamento de Entrada)

Use para publicar serviços internos (TS, WebServer, Câmeras) para a internet.

1. Acesse `Firewall > NAT > Port Forward`.
2. Clique em **Add**.
3. Preencha:
 - * **Interface:** `WAN`
 - * **Protocol:** `TCP` (ou UDP conforme a aplicação).
 - * **Destination port range:** Porta externa (ex: 3389).
 - * **Redirect target IP:** IP interno (ex: `192.168.1.50`).
 - * **Redirect target port:** Porta interna (ex: 3389).

- * **Filter rule association:** `Add associated filter rule` (Isso cria a regra de firewall automaticamente).



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

Etapa 2: Regras de Firewall (LAN/VLANs)

Por padrão, interfaces OPTx (novas VLANs) bloqueiam tudo. É preciso liberar.

1. Acesse `Firewall > Rules > [INTERFACE]`.
2. Clique em **Add** (Seta para cima para colocar no topo).
3. Preencha:
 - * **Action:** `Pass`
 - * **Source:** `[INTERFACE] net` (ex: LAN net).
 - * **Destination:**
 - * `Any` (Para liberar Internet geral).
 - * `! RFC1918` (Alias criado para bloquear acesso a outras VLANs/Redes internas).
4. **Log:** Marque `Log packets that are handled by this rule` se precisar auditar.

Firewall / Rules / WAN / Edit

Action: ✓ Pass

Interface: WAN

Address Family: IPv4

Protocol: TCP

Source: Any

Destination: WAN Address

Destination Port Range: From: 443 (HTTPS) To: 443 (HTTPS)

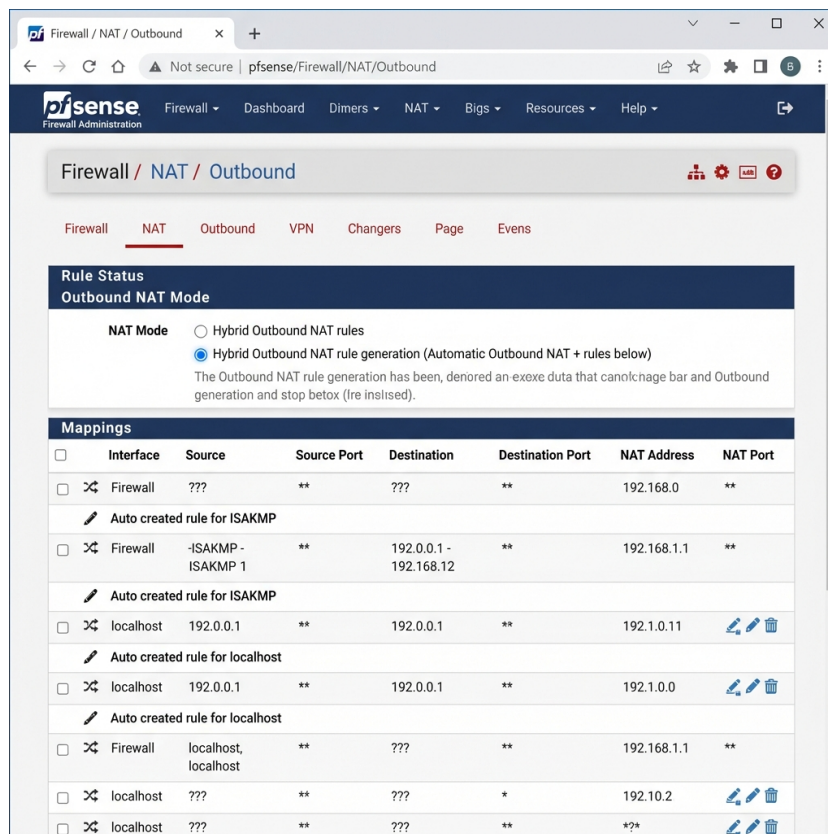
Description: Allow HTTPS Inbound

Save

Etapa 3: Outbound NAT (Para VPNs e MultiWAN)

O modo "Hybrid" é essencial para cenários avançados.

1. Acesse `Firewall > NAT > Outbound`.
2. Mude o **Mode** para `Hybrid Outbound NAT rule generation`.
3. Salve.
4. Crie regras manuais aqui se precisar que uma VLAN saia por um IP específico (ex: SMTP server).



5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: Porta redirecionada (NAT) não abre externamente

- * **Causa:** ISP com CGNAT ou regra de firewall bloqueando.
- * **Solução:**
 1. Verifique se o IP da WAN é público (não começa com 100.x, 10.x, 192.168.x).
 2. Verifique se a opção "Block private networks" está desmarcada na interface WAN.
 3. Use o `Packet Capture` na WAN filtrando pela porta para ver se o pacote chega.

Problema 2: NAT Reflection não funciona (Acesso interno pelo IP externo falha)

- * **Solução:** Habilite `System > Advanced > Firewall & NAT > NAT Reflection mode for port forwards` como `Pure NAT`.

6. DADOS TÉCNICOS

Campo	Valor	Descrição
NAT Reflection	Pure NAT	Recomendado
Max Table Entries	400000	Aumente se tiver muitos conexões

7. VALIDAÇÃO FINAL (Definição de Pronto)

- ☐ O serviço publicado é acessível via 4G (externamente)?
- ☐ O computador na LAN navega?
- ☐ O computador na LAN consegue acessar o serviço pelo IP externo (Loopback)?