



FILTRO DE CONTEÚDO E SEGURANÇA (PFBLOCKERNG)

Guia Oficial iT Guys

Código: ITGENG 0022/26 | **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

Implementar proteção avançada de rede utilizando o **pfBlockerNG-devel**, focando em bloqueio de IPs maliciosos (GeoIP), controle de acesso por países e filtragem de conteúdo web (Ads/Trackers/Sites Maliciosos) via DNSBL.

3. PRÉ-REQUISITOS

- [] pfSense com acesso à internet estável.
- [] Serviço DNS Resolver (Unbound) ativado (ver `Manual 08`).
- [] Chave de Licença MaxMind (Gratuita) para GeoIP.

4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: Instalação do Pacote

1. Acesse `System > Package Manager > Available Packages`.
2. Pesquise por **pfBlockerNG-devel** (Sempre use a versão `devel` pois é a mais atualizada e estável para produção).
3. Clique em **Install** e confirme.
4. Aguarde o término da instalação.

Etapa 2: Setup Wizard (Configuração Inicial)

1. Acesse `Firewall > pfBlockerNG`.
2. O Wizard deve abrir automaticamente. Clique em **Next**.
3. **Inbound/Outbound Interface:**
 - * **Inbound:** `WAN` (Onde os ataques chegam).
 - * **Outbound:** `LAN` (De onde os usuários saem).
4. **VIP Address:** Deixe o padrão (`10.10.10.1`). Este IP virtual serve um "pixel transparente" para páginas bloqueadas HTTP.
5. **Finish.** O sistema fará o primeiro download das listas.

Etapa 3: Configuração Geral e MaxMind

1. Acesse `Firewall > pfBlockerNG > General`.
2. Marque **Enable pfBlockerNG**.
3. **CRON Settings:** Defina para `Every 4 hours` ou `Once a day` (Evite atualizações muito frequentes para não ser banido das listas).
4. Role até **MaxMind GeoIP Configuration:**
 - * Copie sua chave de licença da MaxMind.
 - * Cole no campo **MaxMind License Key**.
 - * Clique em **Save**.
5. Vá na aba **Update** e clique em **Run (Reload) > All** para baixar o banco de dados geográfico.

NOTA

Nota: O layout da tela General contém as opções de CRON e License Key.

Etapa 4: Bloqueio GeoIP (Países)

Use para bloquear tráfego de países com alto índice de ataques (ex: China, Rússia) se sua empresa não faz negócios lá.

1. Acesse `Firewall > pfBlockerNG > IP > GeoIP`.
2. Escolha uma categoria (ex: **Top_Spammers**).
3. No painel direito (List), selecione os países desejados ou "Select All".
4. **Action:**
 - * **Deny Inbound:** Bloqueia quem tenta entrar (Protege seus serviços publicados).
 - * **Deny Both:** Bloqueia entrada e saída (Impede que um malware interno se comunique com C2 nesses países).

5. Clique em **Save**.

Etapa 5: DNSBL (Filtro de Conteúdo/Ads)

Use para bloquear anúncios, rastreadores e sites adultos.

1. Acesse `Firewall > pfBlockerNG > DNSBL`.
2. **DNSBL Mode:** `Unbound Python Mode` (Melhor performance e report de memória).
3. **Permit Firewall Rules:** Selecione as redes (LAN, VLANs) onde o bloqueio deve atuar.
4. **DNSBL Groups:**
 - * O pacote já vem com o grupo **EasyList** (Adblock padrão).
 - * Adicione feeds personalizados em `Firewall > pfBlockerNG > Feeds`.
5. **SafeSearch:** (Opcional) Marque para forçar Google/Bing/YouTube em modo restrito.
6. Salve e force um **Reload** na aba **Update**.

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: WebGUI lenta após ativar pfBlockerNG

- * **Causa:** DNSBL consumindo muita RAM ou CPU ao carregar listas gigantes.
- * **Solução:** Reduza o número de listas, ative o `Unbound Python Mode` ou aumente a RAM da VM/Hardware.

Problema 2: Site legítimo bloqueado (Falso Positivo)

- * **Causa:** Domínio está em alguma blacklist (ex: `googleadservices.com` bloqueado impede clique em anúncios do Google Shopping).
- * **Solução:**
 1. Acesse `Firewall > pfBlockerNG > Reports > Unified`.
 2. Identifique o domínio bloqueado (em vermelho).
 3. Clique no ícone + (Whitelist) ao lado do domínio.
 4. O domínio será adicionado à Whitelist personalizada e liberado imediatamente (Unbound Python Mode) ou após Reload.

Problema 3: Falha no download MaxMind

- * **Causa:** Chave de licença inválida ou erro de conexão.
- * **Solução:** Verifique os logs em `Firewall > pfBlockerNG > Logs > error.log`. Garanta que a chave da MaxMind é a versão correta (v3.1.1+).

6. DADOS TÉCNICOS

Campo	Valor	Descrição
VIP Padrão	10.10.10.1	WebServer de Bloqueio
Portas VIP	80/443	Portas WebServer
Cron	4/12/24h	Frequência de Update

7. VALIDAÇÃO FINAL (Definição de Pronto)

- ☐ Widget do pfBlockerNG no Dashboard mostra status das listas (Verde)?
- ☐ Teste de acesso a sites de Ads (ex: doubleclick.net) falha ou é redirecionado para o VIP?
- ☐ O banco de dados GeoIP foi baixado com sucesso?