DIAGNÓSTICO AVANÇADO, SHELL E RECOVERY

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - DIAGNÓSTICO AVANÇADO, SHELL E RECOVERY

Código: ITGENG 0026/26 | **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

Fornecer ferramentas e comandos avançados para diagnóstico de rede, performance e recuperação de desastres no pfSense, focando no uso do Shell (`pfctl`, `tcpdump`) quando a WebGUI está inacessível ou insuficiente.

3. PRÉ-REQUISITOS

[ ] Acesso SSH habilitado (`System > Advanced > Admin Access`).
[ ] Usuário `admin` ou `root` com senha conhecida.
[ ] Acesso físico (Console/VGA/Serial) para casos de recuperação crítica.

4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: Comandos Essenciais do Shell (SSH/Console)

Se a interface gráfica travar, use o shell (Opção 8 no menu console).

1. Gerenciamento do Filtro de Pacotes (pf)

- `pfctl -d`: **Desabilita** o Firewall temporariamente (CUIDADO! Libera tudo). Use se trancou para fora.
- `pfctl -e`: **Habilita** o Firewall novamente.
- `pfctl -f /etc/filter.conf`: Recarrega as regras de filtro.
- `pfctl -s info`: Mostra estatísticas gerais (Estado, Drops).

2. Diagnóstico de Interface e Roteamento

- `ifconfig`: Lista interfaces, IPs e MACs.
- `netstat -rn`: Mostra a tabela de roteamento.
- `netstat -i`: Mostra estatísticas de erros/colisões por interface.

3. Captura de Pacotes (tcpdump)

Ferramenta definitiva para ver o que está passando no cabo.

- `tcpdump -i em0`: Vê tudo na interface `em0`.
- `tcpdump -i em0 host 192.168.1.50`: Vê tráfego de/para um IP específico.
- `tcpdump -i em0 port 80`: Vê apenas tráfego HTTP.
- `tcpdump -n -e -ttt -i pflog0`: Vê o log do firewall em tempo real (o que está sendo bloqueado).

Etapa 2: Recuperação de Desastres (Rescue)

Cenário: Perdi a senha de admin ou lockout da WebGUI.

1. [x] Acesse o **Console Físico** (Monitor+Teclado ou Serial).
2. [x] No menu numérico (0-16):

- **Opção 3 (Reset webConfigurator password):** Reseta senha para `pfsense`.
- **Opção 4 (Reset to factory defaults):** Zera TUDO. (Use em último caso).
- **Opção 11 (Restart webConfigurator):** Reinicia apenas o serviço PHP/Nginx. Use se a GUI estiver dando erro 502/504.
- **Opção 15 (Restore recent configuration):** Permite voltar para um backup automático anterior. O pfSense salva backups a cada alteração. Isso salva vidas!

Etapa 3: Diagnóstico via WebGUI (Tools)

Se a GUI funciona, use:

1. [x] **Test Port (`Diagnostics > Test Port`):**
- Testa se uma porta TCP está aberta num servidor remoto. Melhor que ping para testar serviço.
2. [x] **Packet Capture (`Diagnostics > Packet Capture`):**
- Interface gráfica para o `tcpdump`. Permite baixar o arquivo `.cap` para analisar no Wireshark do seu PC.
3. [x] **States Dump (`Diagnostics > States`):**
- Veja quem está conectado, quantos bytes consumiu e mate conexões específicas.

Etapa 4: Logs do Sistema

Caminhos importantes no Shell para leitura com `tail -f`:

- `/var/log/system.log`: Log geral do sistema.
- `/var/log/filter.log`: Logs do Firewall (Blocos/Pass).
- `/var/log/dhcpd.log`: Logs do DHCP.
- `/var/log/openvpn.log`: Logs das VPNs.
- `/var/log/nginx.log`: Logs do servidor web da GUI.

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: "PHP ERROR: Type: 1, File: /etc/inc/..."

- **Causa:** Corrupção de arquivos ou disco cheio.
- **Solução:**

1. [x] Verifique espaço em disco: `df -h`.

2. [x] No console, escolha **Opção 16 (Restart PHP-FPM)**.
3. [x] Se persistir, reforce update via console opção 13.

Problema 2: Alta Latência / Perda de Pacotes

• **Causa:** Hardware insuficiente (Mbuf exhaustion) ou loop de rede.

• **Solução:**

1. [x] Verifique uso de CPU (`top -aSH`).
2. [x] Verifique interrupções (`vmstat -i`). Se uma placa de rede gera 20k+ interrupts, pode ser defeito ou driver ruim.
3. [x] Aumente Mbufs em `System > Advanced > Networking` se tiver RAM sobrando.

Problema 3: Boot Loop ou Filesystem Error

• **Solução:**

1. [x] Boot no modo Single User (`s` no boot loader).
2. [x] Execute `fsck -y /` para corrigir o sistema de arquivos (apenas UFS). ZFS geralmente se autocorrige ou exige scrub.

6. DADOS TÉCNICOS

Comando	Função	Exemplo
pfctl -d	**Desativa Firewall**	**Emergência**
viconfig	**Edita config.xml**	**Uso Avançado**
top	**Monitor de Processos**	**Ver carga**

7. VALIDAÇÃO FINAL (DEFINIÇÃO DE PRONTO)

[ ] Consegue acessar via SSH?
[ ] O comando `tcpdump` mostra tráfego?
[ ] Sabe onde restaurar um backup pelo console (Opção 15)?
[ ] Logs estão acessíveis e legíveis?