IDS/IPS COM SURICATA

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - IDS/IPS COM SURICATA

Código: ITGENG 0023/26 | **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

Implementar Sistema de Detecção e Prevenção de Intrusão (IDS/IPS) usando Suricata no pfSense para monitorar, detectar e bloquear tráfego malicioso (exploits, malware C2, scanners) em tempo real, utilizando análise de assinaturas e comportamento.

3. PRÉ-REQUISITOS

[ ] pfSense com hardware adequado (Mínimo 4GB RAM recomendado, CPU multi-core).
[ ] **Snort VRT Oinkmaster code** (Grátis, cadastro no snort.org) ou **Emerging Threats Open** (Não requer cadastro).
[ ] Conhecimento das redes internas para evitar bloqueio falso positivo.

4. PASSO A PASSO (EXECUÇÃO)

Etapa 1: Instalação do Pacote

1. [x] Acesse `System > Package Manager > Available Packages`.
2. [x] Pesquise por **suricata**.
3. [x] Clique em **Install** e confirme.

Etapa 2: Configuração Global e Updates

1. [x] Acesse `Services > Suricata > Global Settings`.
2. [x] **Install ETOpen Emerging Threats rules:** Marque (Fontes abertas e excelentes).
3. [x] **Install Snort VRT rules:** (Opcional) Requer Oinkmaster code.
4. [x] **Update Interval:** `12-Hours`.
5. [x] **Remove Blocked Hosts Interval:** `1 Hour` (Importante para não bloquear IPs legítimos para sempre em caso de falso positivo).

6. [x] Clique em **Save**.
7. [x] Vá na aba **Updates** e clique em **Update** para baixar as regras iniciais.

Etapa 3: Criar Interface de Monitoramento

1. [x] Acesse `Services > Suricata > Interfaces`.
2. [x] Clique em **Add**.
3. [x] **Interface:** Selecione a interface física (ex: `WAN`).

> **Nota:** Monitorar a WAN vê todos os ataques (muito ruído). Monitorar a LAN vê apenas o que passou pelo Firewall ou ameaças internas (menos ruído, mais foco em clientes infectados). Recomendação: Comece pela WAN em modo IDS (apenas alerta).

4. [x] **Enable:** Marque para ativar.
5. [x] **Block Offenders:** Marque se quiser que o Suricata bloqueie o IP (IPS Mode).

• *Sugestão:* Deixe desmarcado na primeira semana para aprender o tráfego (IDS Mode).
• **Kill States:** Marque para derrubar conexões ativas imediatamente.

Etapa 4: Seleção de Categorias de Regras

1. [x] Dentro da edição da Interface, vá na aba **Categories**.
2. [x] Clique em **Select All** (Cuidado com RAM/CPU) ou escolha categorias críticas:

• `emerging-exploit` (Exploits conhecidos)
• `emerging-malware` (Malware C2 activity)
• `emerging-mobile_malware`
• `emerging-scan` (Portscanners)
• `emerging-trojan`

3. [x] Evite categorias como `emerging-info` ou `emerging-chat` em ambientes corporativos se não quiser monitorar uso aceitável, pois geram muito log.
4. [x] Salve.

Etapa 5: Ajuste de SID (Signature ID) e Supressão

Se um alerta legítimo bloquear seu tráfego (falso positivo):

1. [x] Acesse `Services > Suricata > Alerts`.
2. [x] Identifique o alerta (ex: `ET POLICY Python-urllib/2.7`).
3. [x] Para **suprimir** (nunca mais alertar para esse IP/Regra): Clique no ícone de `+` em "Suppress this GID:SID".
4. [x] Para **desativar** a regra globalmente: Clique no ícone de `X` (Disable this SID).
5. [x] A regra irá para a lista de **SID Mgmt** e não incomodará mais.

5. SOLUÇÃO DE PROBLEMAS (TROUBLESHOOTING)

Problema 1: Internet caiu após ativar IPS

• **Causa:** Falso positivo bloqueando DNS (8.8.8.8) ou Gateway.
• **Solução:**

1. [x] Desative o "Block Offenders" na interface temporariamente.
2. [x] Verifique a aba **Blocked** e remova o IP crítico.
3. [x] Adicione os DNS e Gateways numa **Pass List** em `Services > Suricata > Pass Lists` e vincule à interface.

Problema 2: Alta carga de CPU/RAM

- **Causa:** Muitas categorias ativadas ou inspeção profunda em hardware fraco.
- **Solução:** Desative categorias menos críticas (`deleted`, `info`, `games`). Mude o "Run Mode" em Interface Settings para `suro` (High Performance) se disponível.

Problema 3: Suricata não inicia

- **Causa:** Erro no download de regras ou falta de RAM.
- **Solução:** Verifique `Status > System Logs > Suricata`. Tente rodar o update manual das regras novamente.

6. DADOS TÉCNICOS

Campo	Valor	Descrição
Modo	**IDS (Alerta) / IPS (Bloqueio)**	**Inline vs Legacy**
Engine	**Suricata**	**Multi-threaded**
Log	**/var/log/suricata**	**Logs de alerta**

7. VALIDAÇÃO FINAL (DEFINIÇÃO DE PRONTO)

[ ] O serviço está rodando na interface WAN?
[ ] A aba Alerts mostra tentativas de conexão (ex: Portscan)?
[ ] O tráfego legítimo não está impactado?