SAPO-BOI: Pulando a Pilha de Rede no Desenvolvimento de um NIDS Baseado em BPF/XDP

Raphael Kaviak Machnicki, Jorge Correia,
Ulisses Penteado, Vinicius Garcia, André Grégio

Universidade Federal do Paraná
BluePex Security Solutions

Motivação

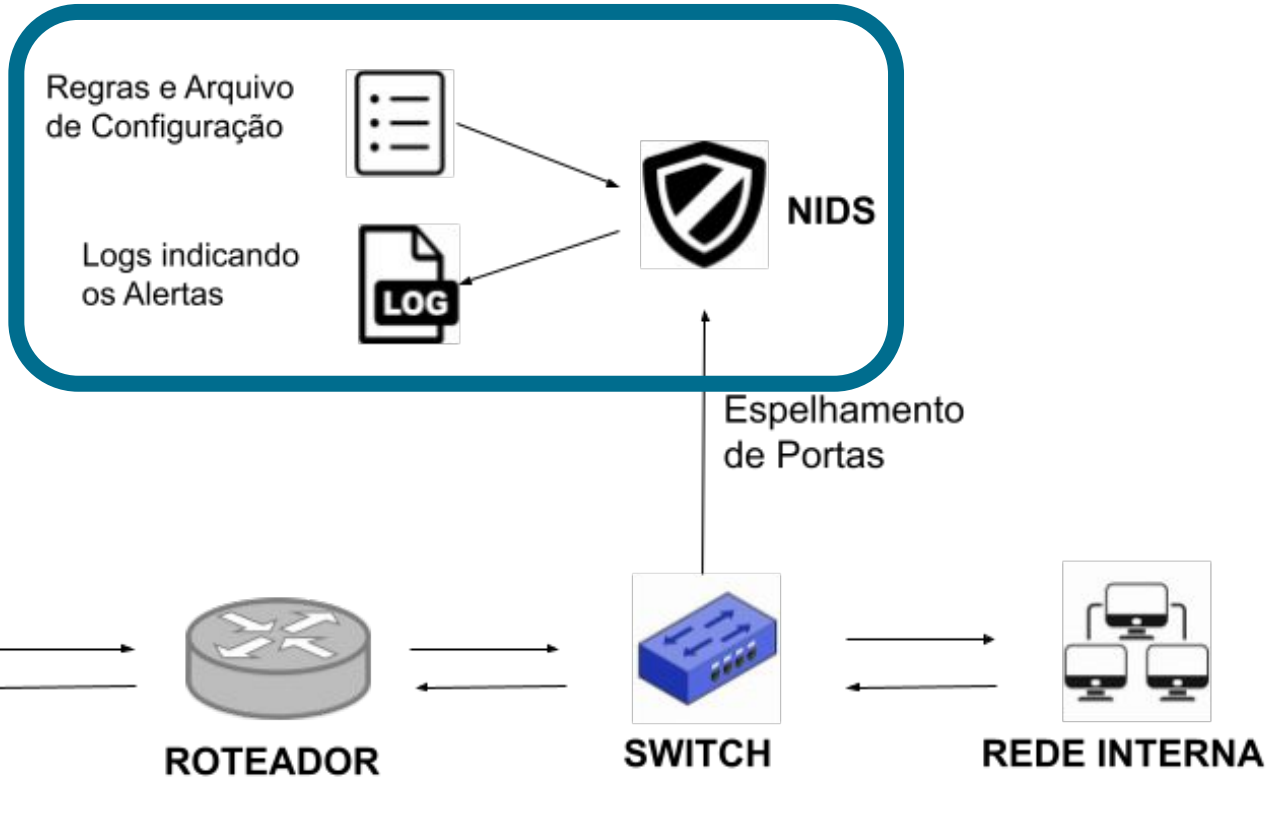
Lei nº 12.737 de 30 de Novembro de 2012

Projeto atualiza Lei Carolina Dieckmann sobre crimes cibernéticos

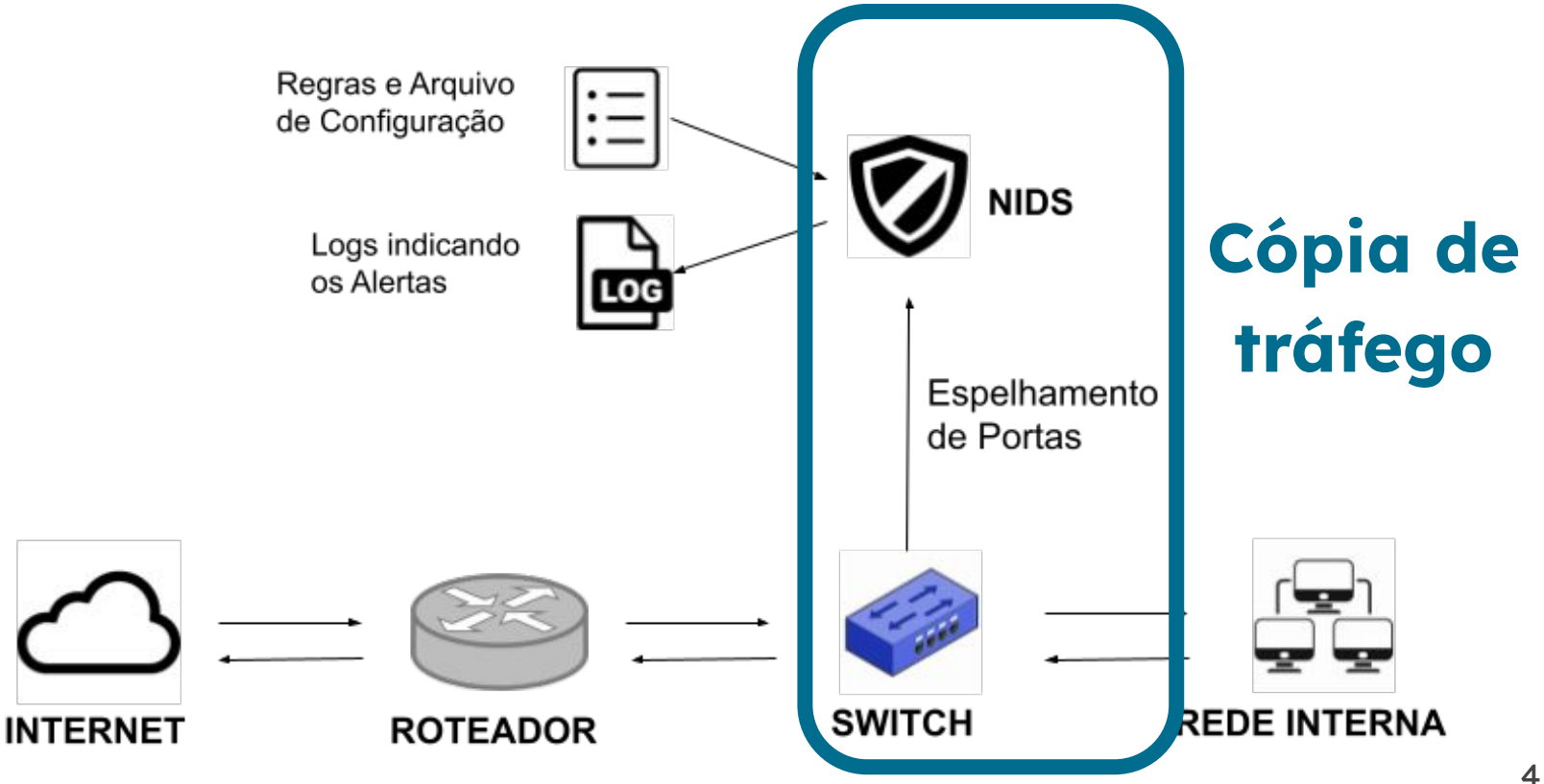
Pergunta: **Como detectar intrusões?**

Sistemas de Detecção de Intrusão em Redes por Assinatura - NIDS

Definição das Assinaturas (Regras)



Sistemas de Detecção de Intrusão em Redes por Assinatura - NIDS



Problemas

NIDS (a 10 Gbps)	# Regras Carregadas	Uso de CPU <Usuário>-<Kernel> (0% a 2000%)	Pacotes Não Avaliados
Snort	8000	1274 - 726	92.4%
	16000	1221 - 779	92.3%
Suricata	8000	1247 - 753	10.5%
	16000	1433 - 474	46.7%

Problemas

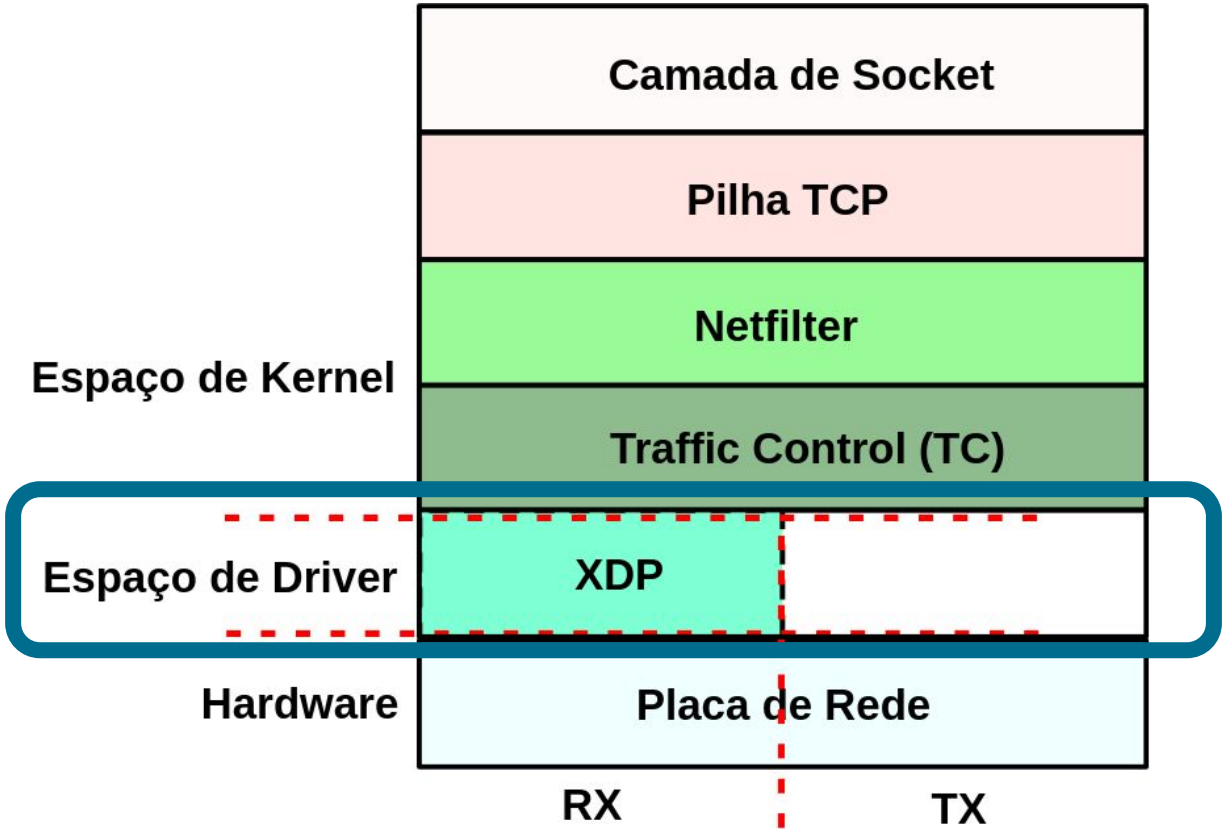
NIDS ***(a 10 Gbps)***	**# Regras Carregadas**	**Uso de CPU <Usuário>-<Kernel> (0% a 2000%)**	**Pacotes Não Avaliados**
Snort	8000	1274 - 726	92.4%
	16000	1221 - 779	92.3%
Suricata	8000	1247 - 753	10.5%
	16000	1433 - 474	46.7%

Desafio

Pergunta: **Como permitir que mais pacotes sejam avaliados pelo sistema?**

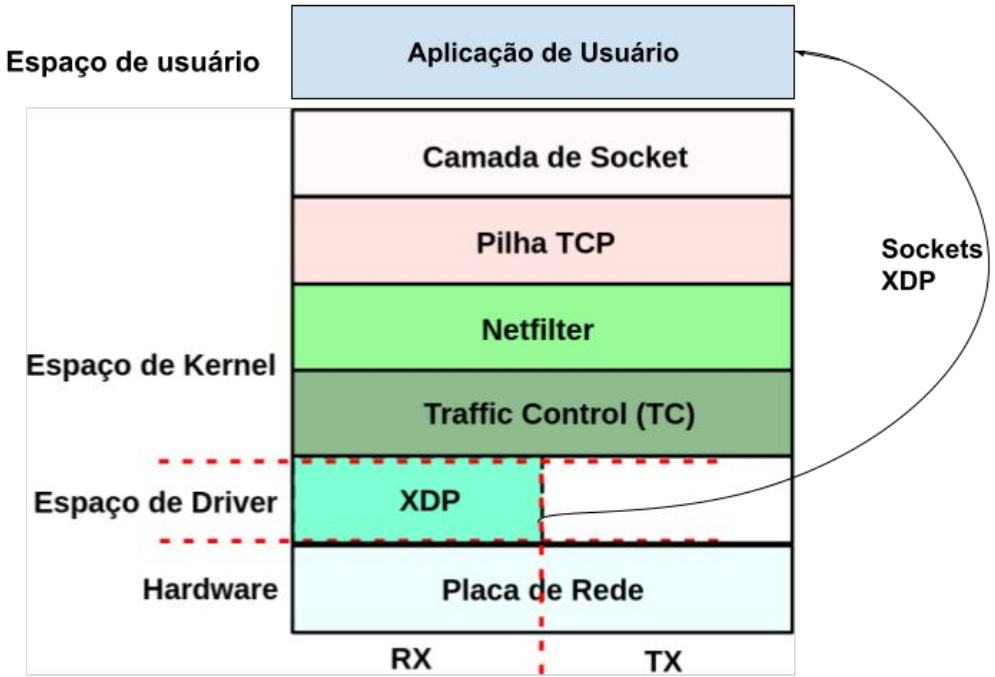
- XDP
- Gancho para programas BPF

XDP

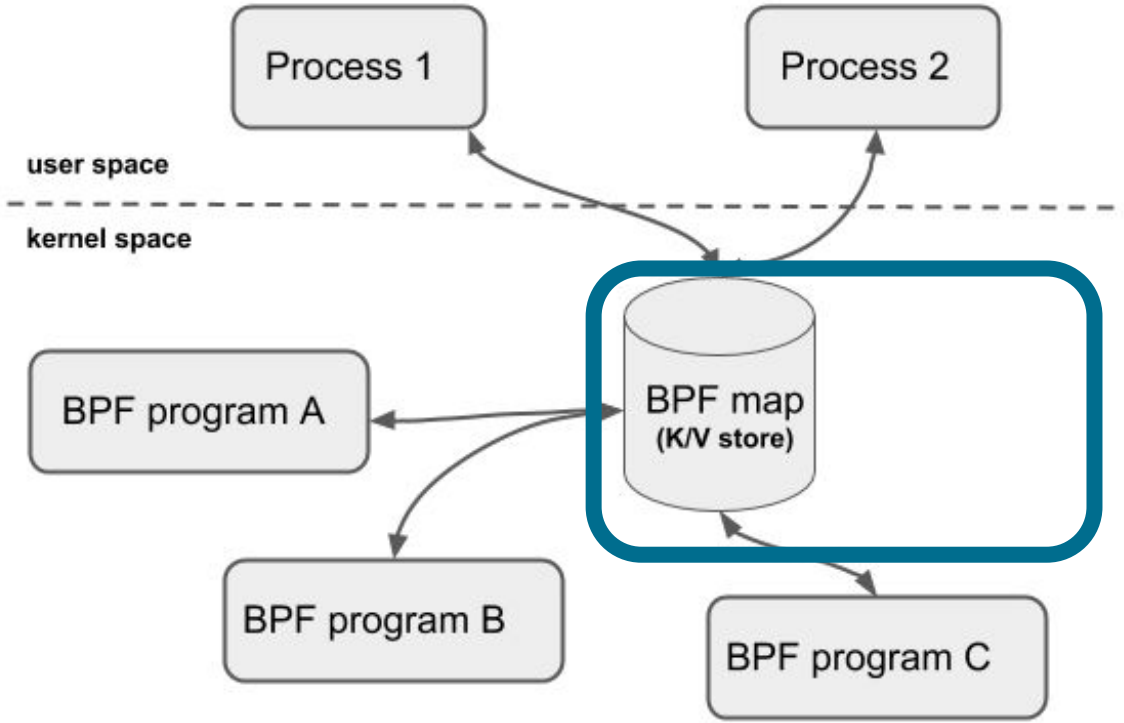


Pacotes avaliados ainda em espaço de driver

Pulando a Pilha de Rede



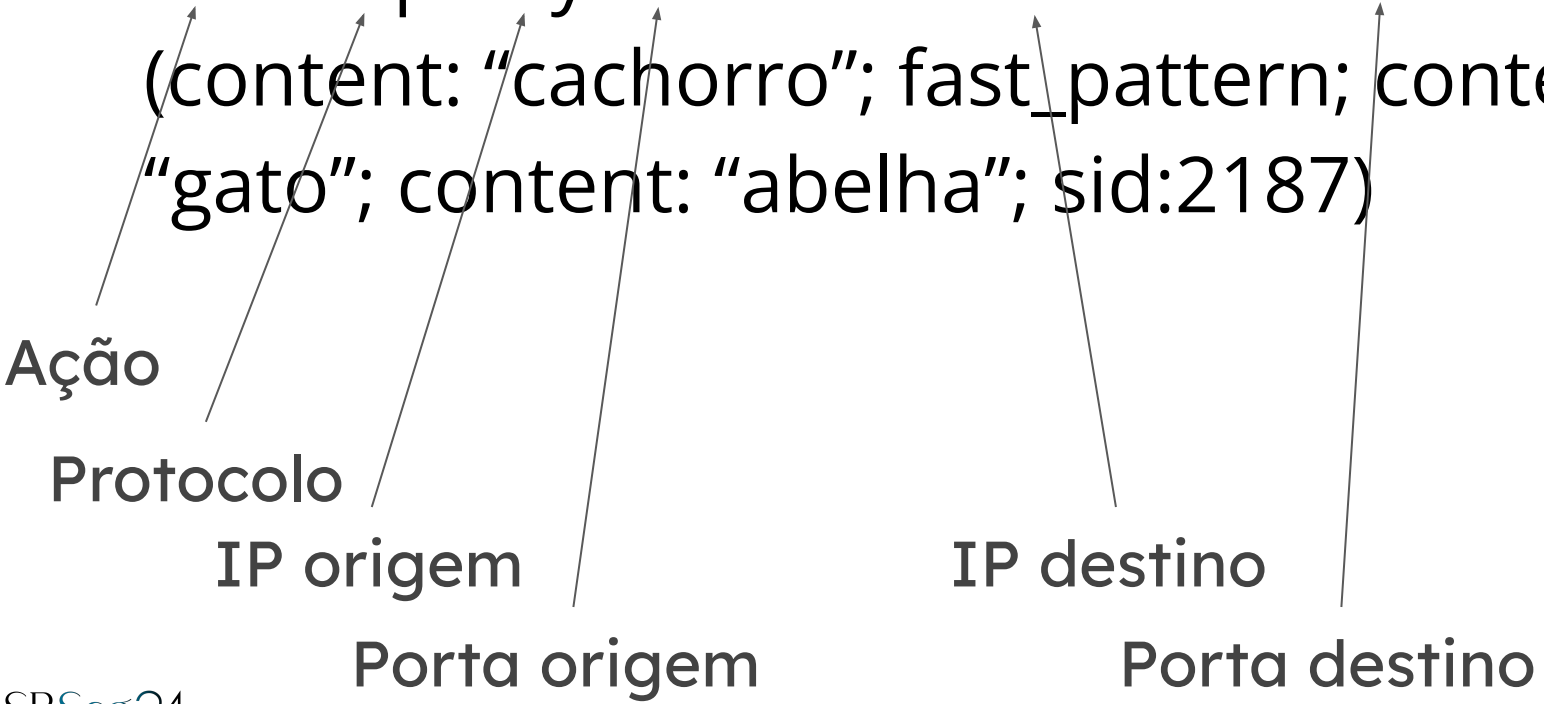
Programas BPF e IPC via Mapas



Mapas BPF provém Comunicação entre processos de espaços de usuário e kernel

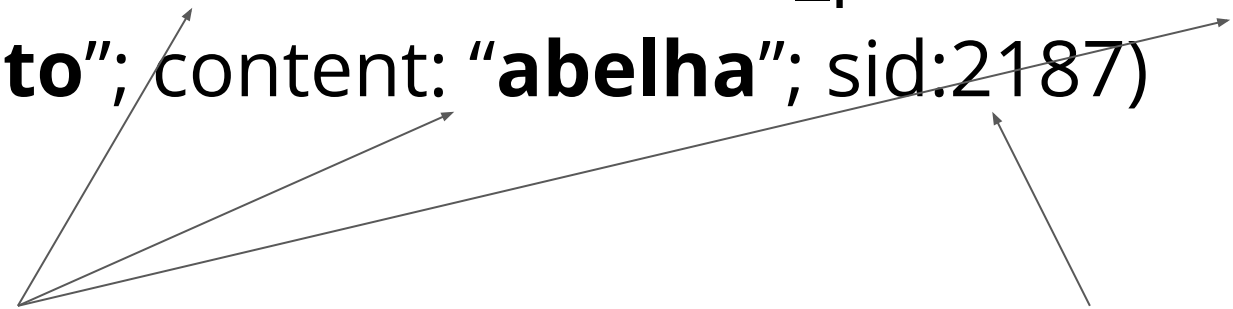
Regras de NIDS

- alert tcp any **25** -> 192.168.26.59 **44** (content: “cachorro”; fast_pattern; content: “gato”; content: “abelha”; sid:2187)



Regras de NIDS

- alert tcp any 25 -> 192.168.26.59 44 (content: “**cachorro**”; fast_pattern; content: “**gato**”; content: “**abelha**”; sid:2187)

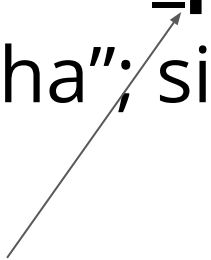


Padrões a ser procurados

Identificador da regra

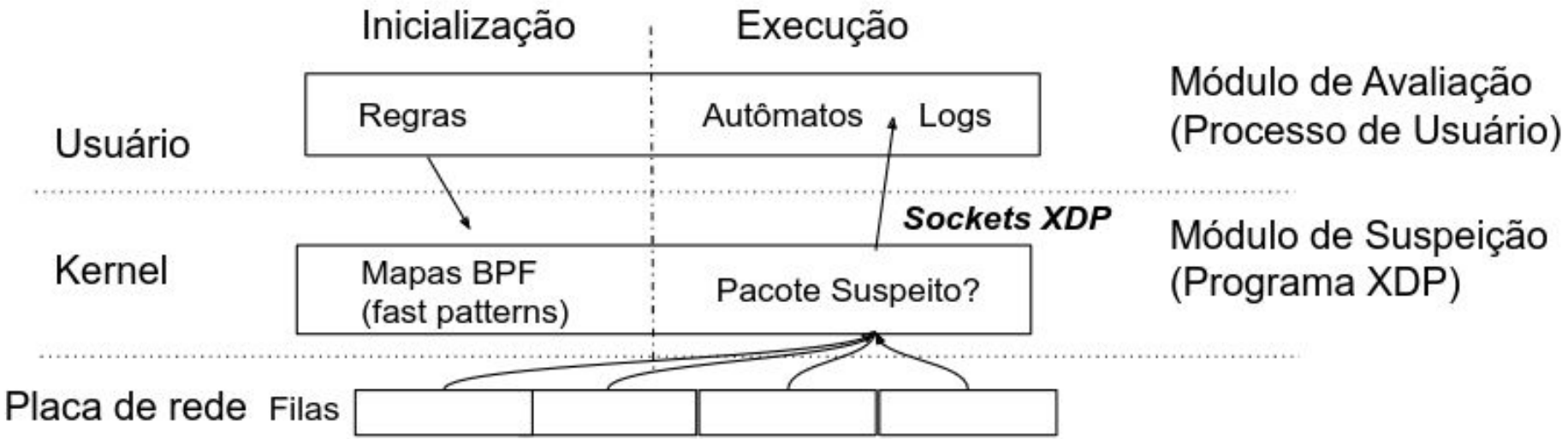
Regras de IDS - fast patterns

- alert tcp any 25 -> 192.168.26.59 44 (content: “cachorro”; **fast_pattern**; content: “gato”; content: “abelha”; sid:2187)

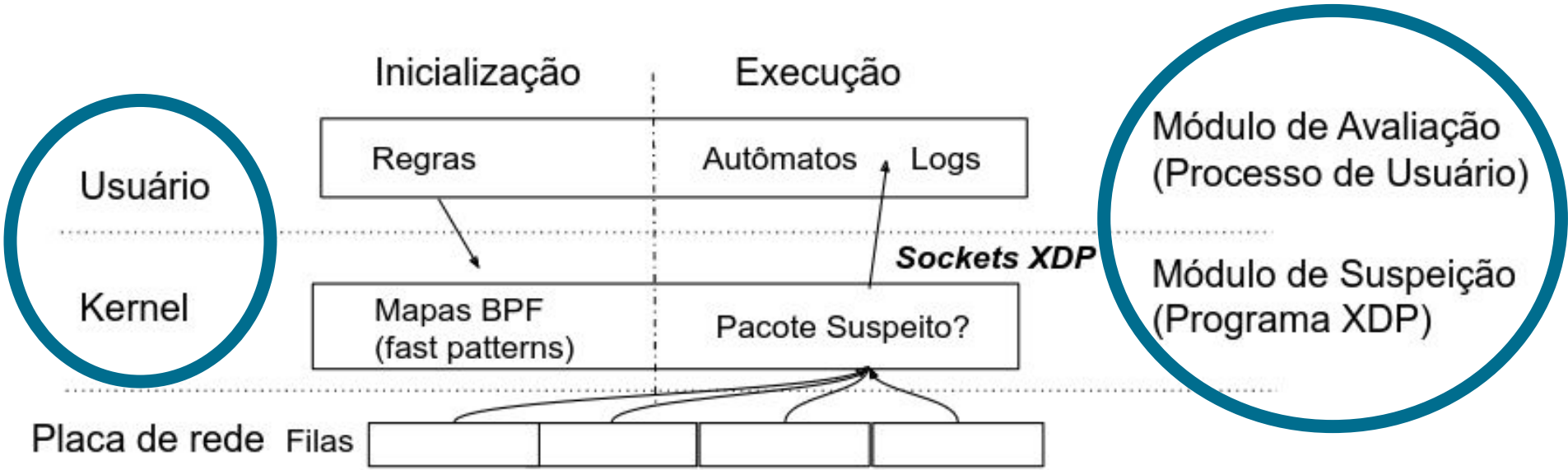


Modificador para melhoria de desempenho!

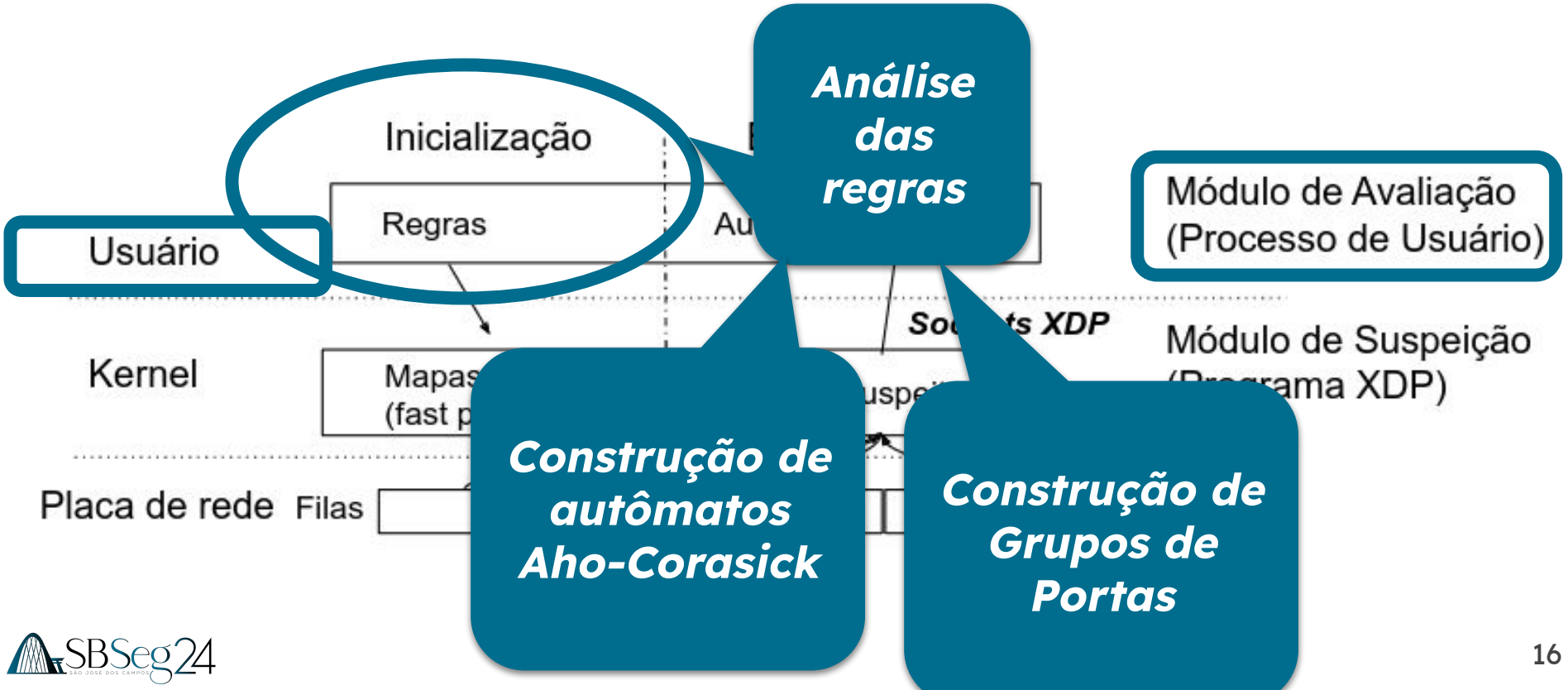
Solução Proposta -> SAPO-BOI



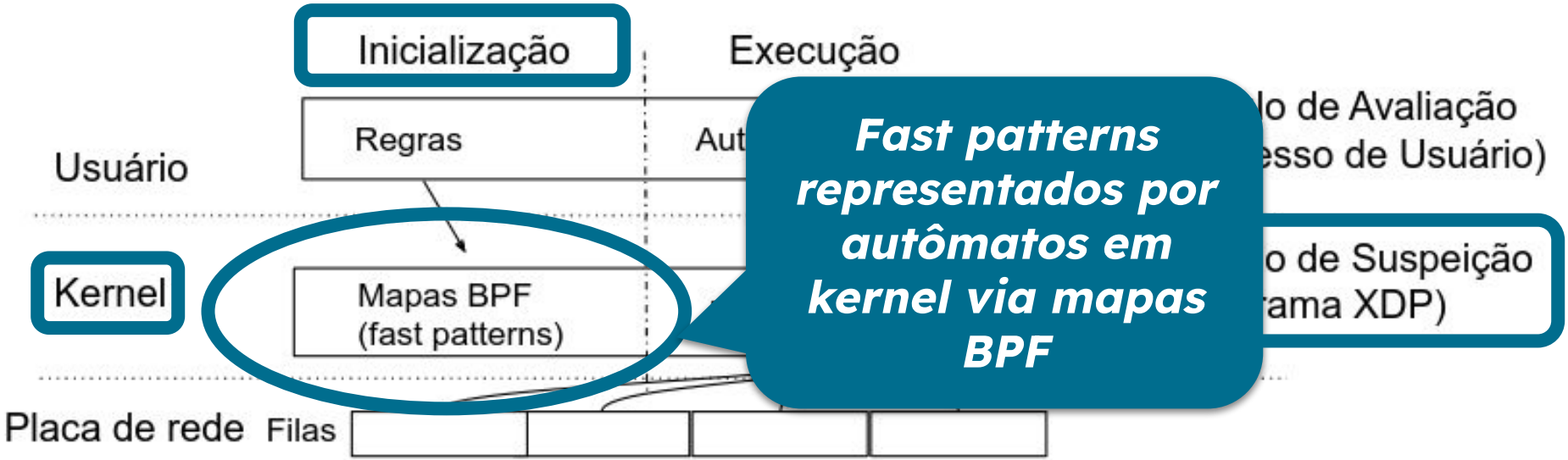
Solução Proposta



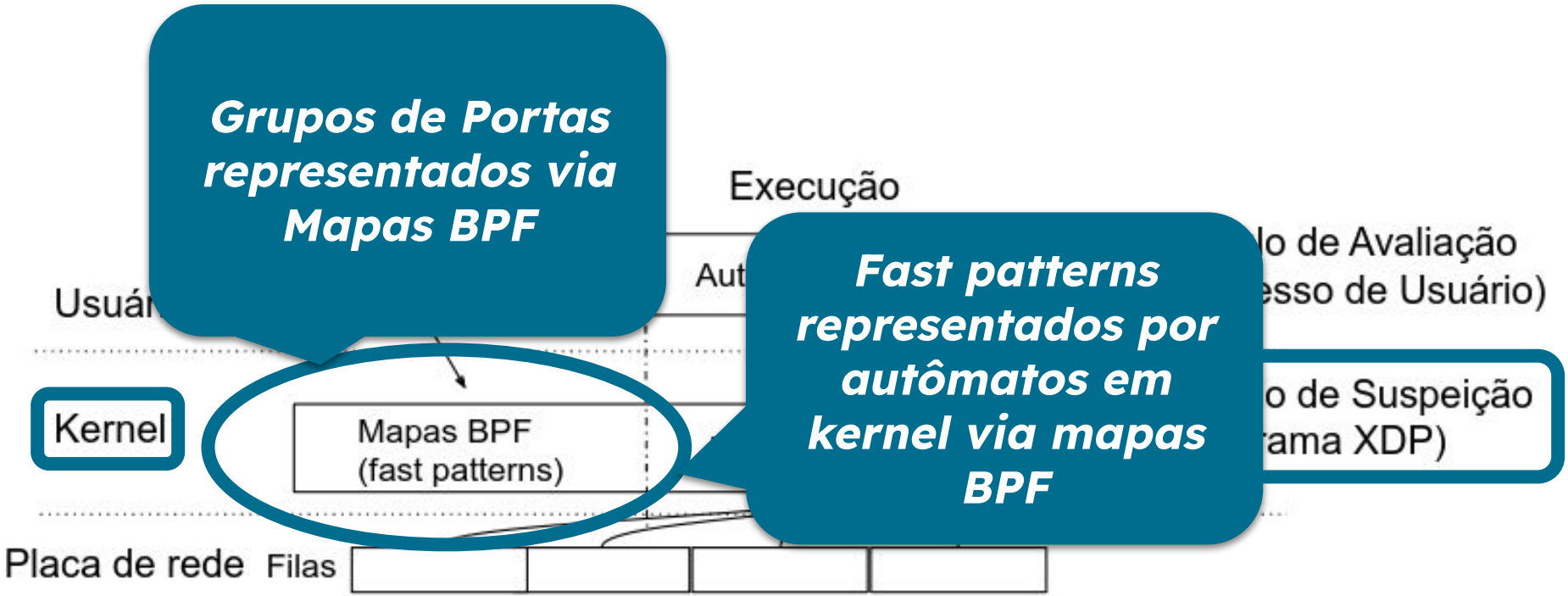
Solução Proposta



Solução Proposta

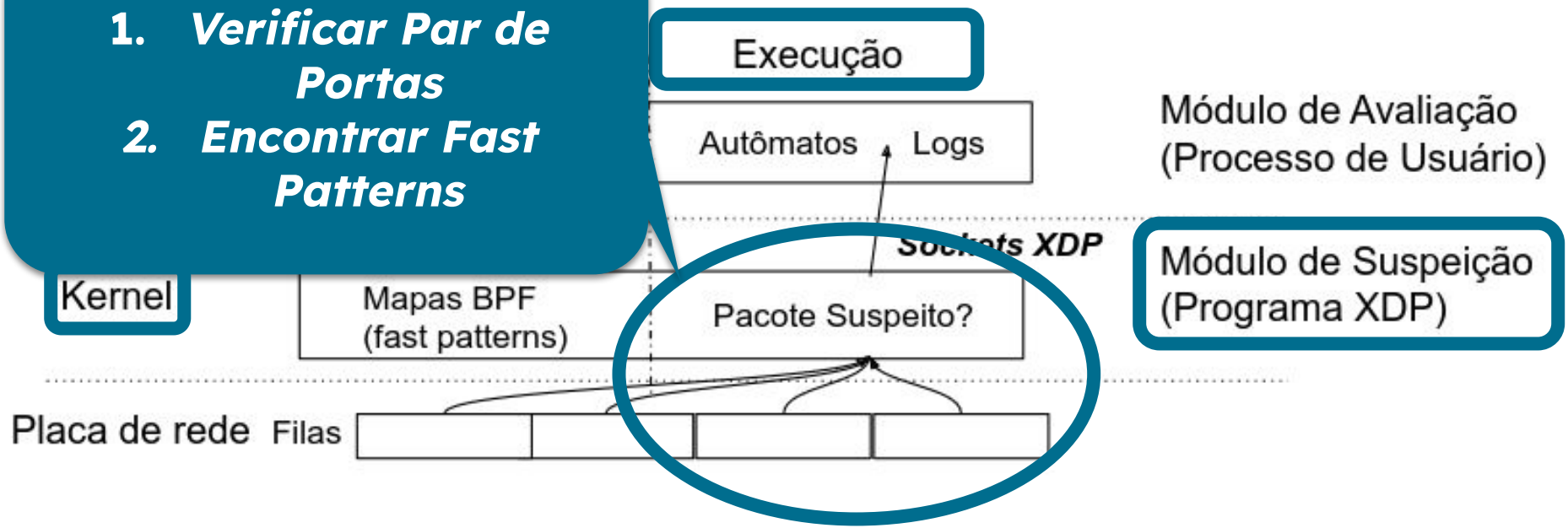


Solução Proposta

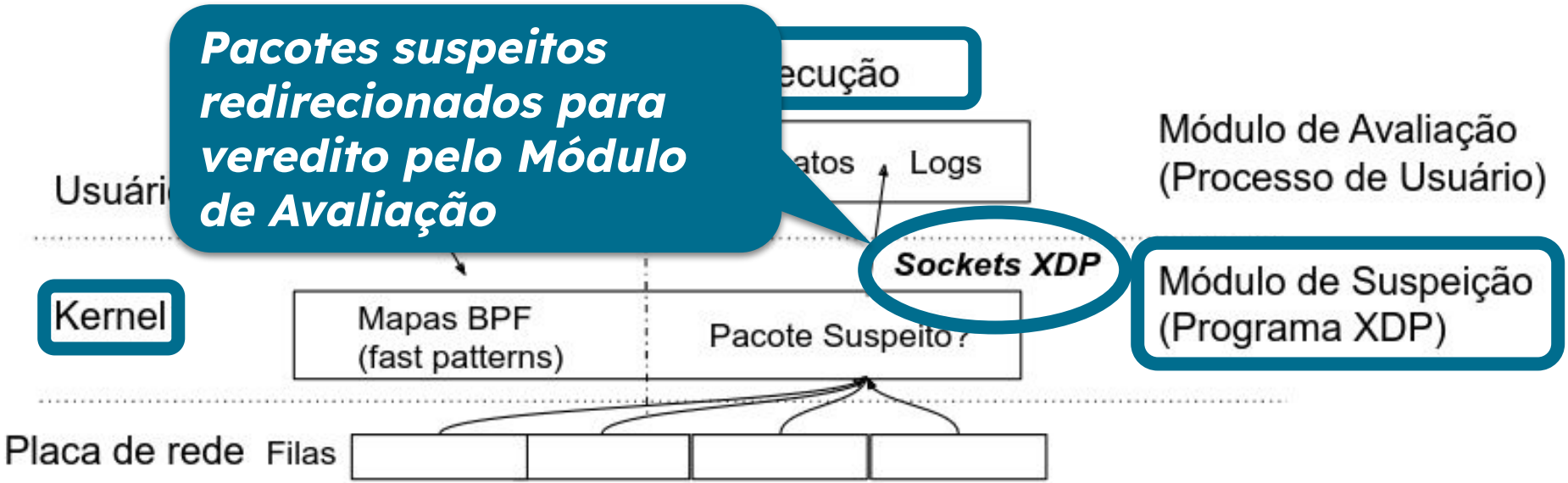


Solução Proposta

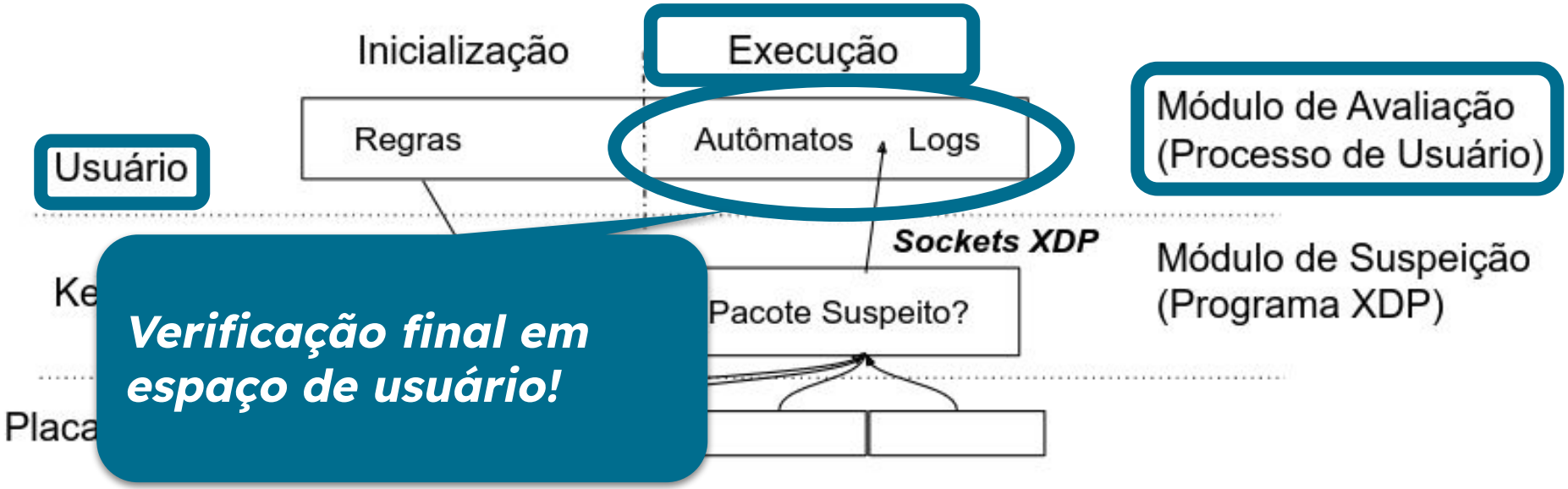
1. ***Verificar Par de Portas***
2. ***Encontrar Fast Patterns***



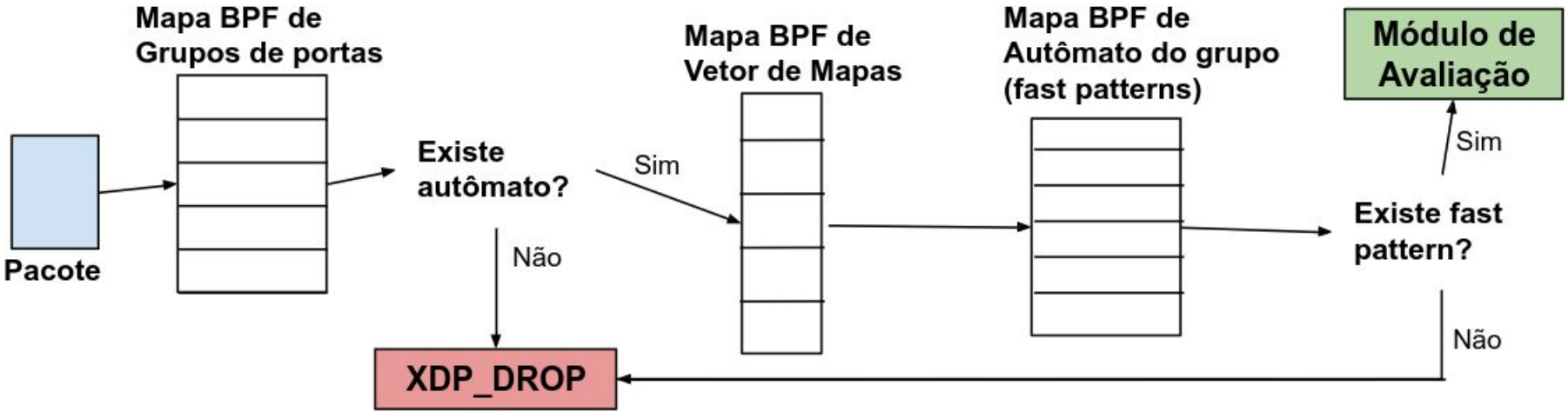
Solução Proposta



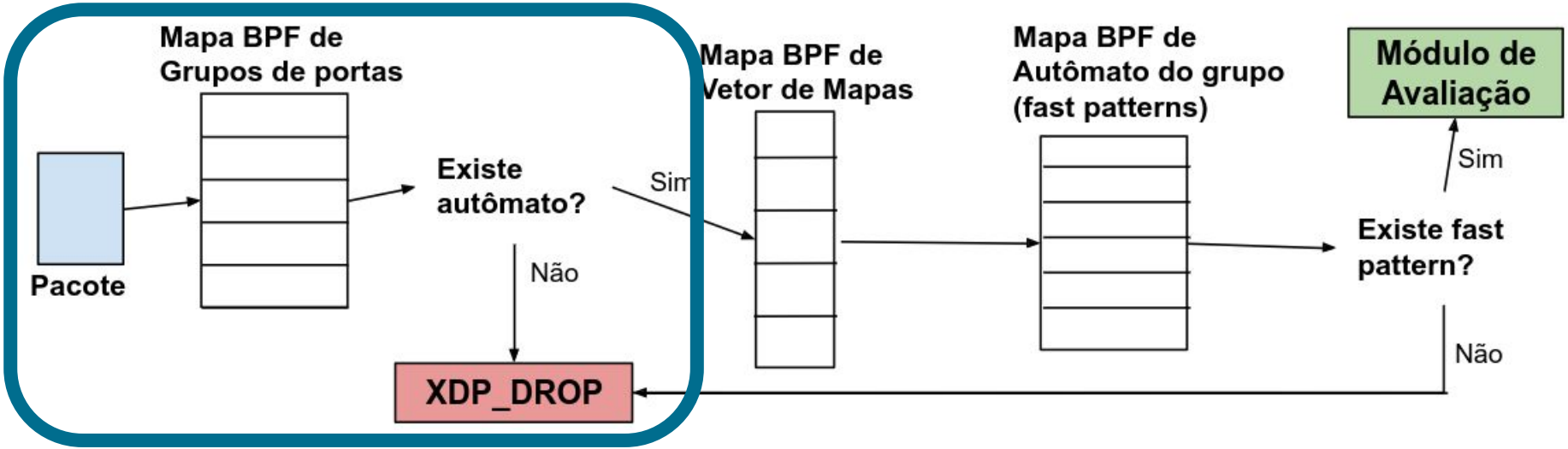
Solução Proposta



Solução Proposta - Módulo de Suspeição

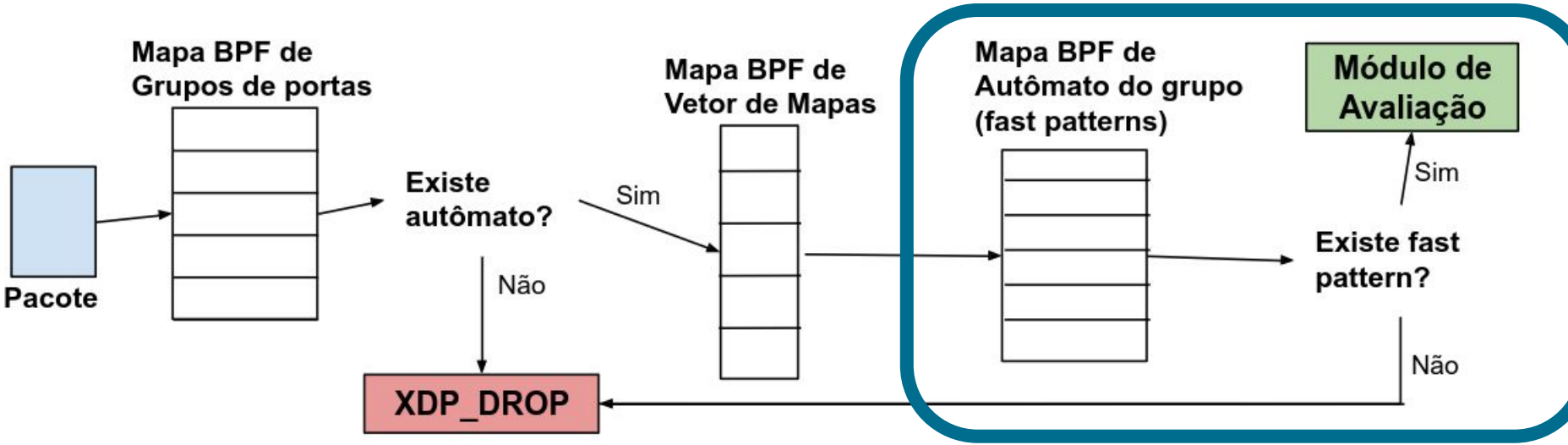


Solução Proposta - Módulo de Suspeição



Verificação do par de portas

Solução Proposta - Módulo de Suspeição



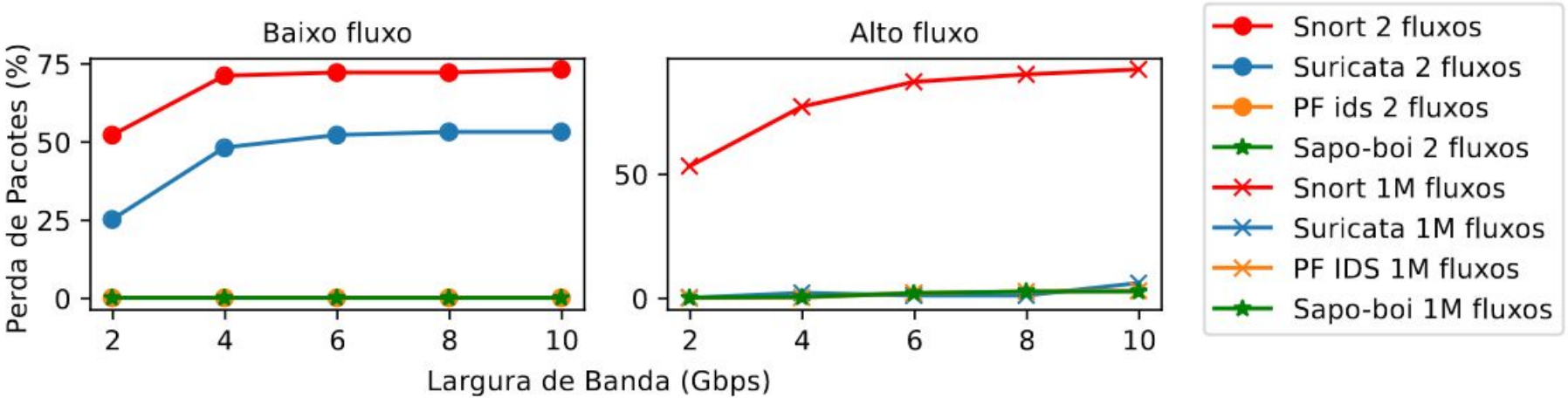
Verificação do Autômato AC

Avaliação

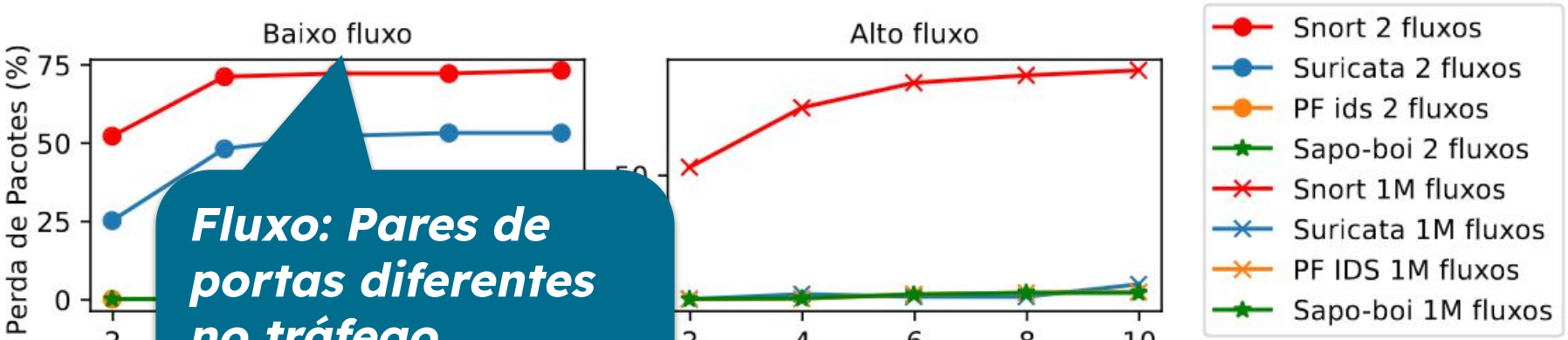
4 Soluções:

- SAPO-BOI (Kernel -> Sockets XDP)
- PF IDS (Kernel -> Perf Events)
- Snort (Usuário)
- Suricata (Usuário)

Avaliação - Pacotes Analisados

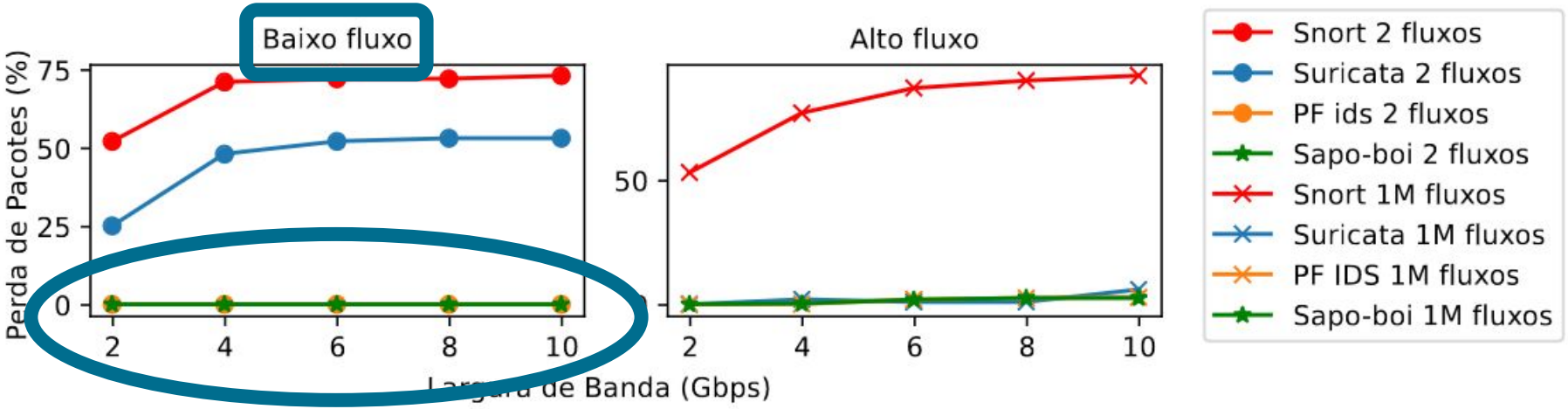


Avaliação - Pacotes Analisados



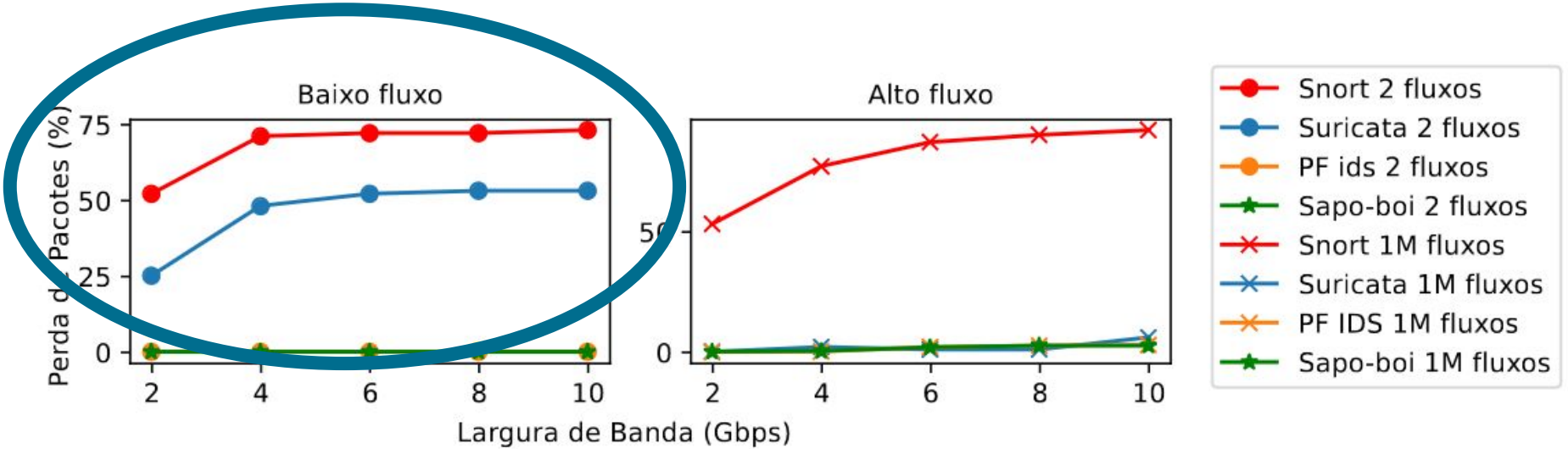
Fluxo: Pares de portas diferentes no tráfego. Tráfego não malicioso!

Avaliação - Pacotes Analisados



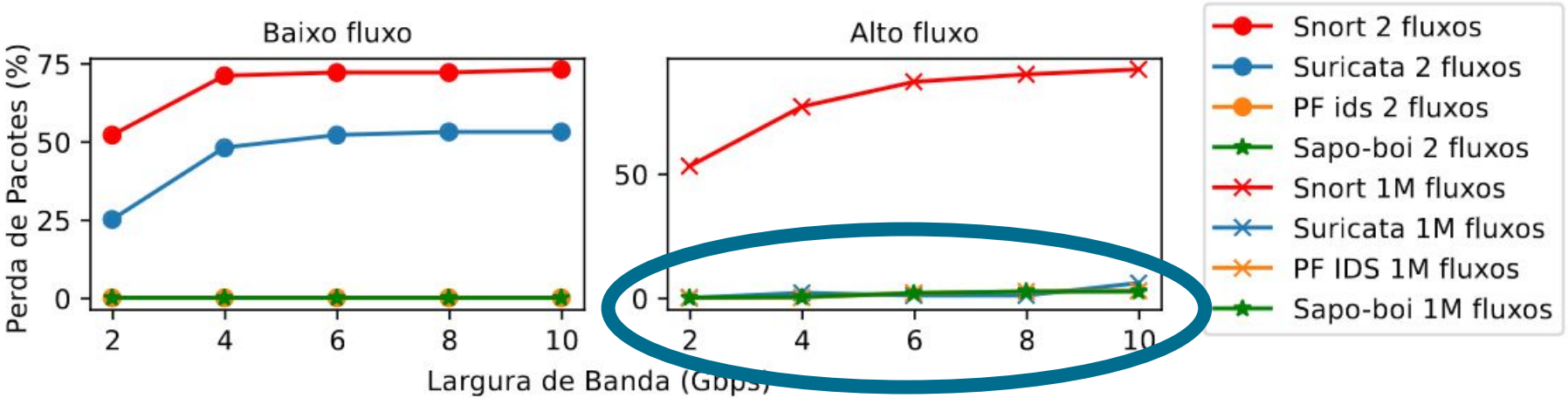
Perda zero em kernel

Avaliação - Pacotes Analisados



Perdas: 50% para Suricata
e 75% para Snort

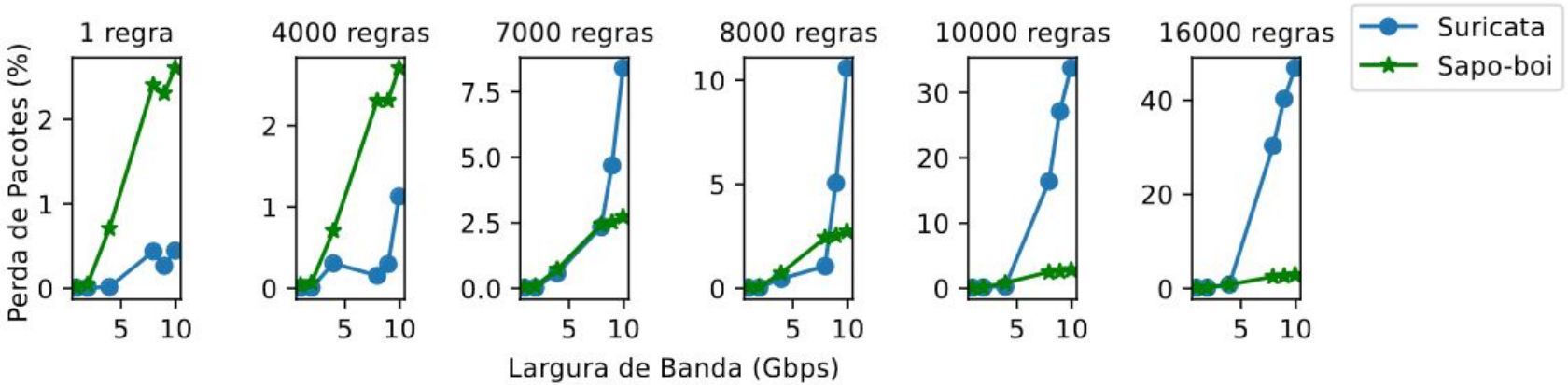
Avaliação - Pacotes Analisados



Perdas: 2,7% para IDS em Kernel e 5% para Suricata

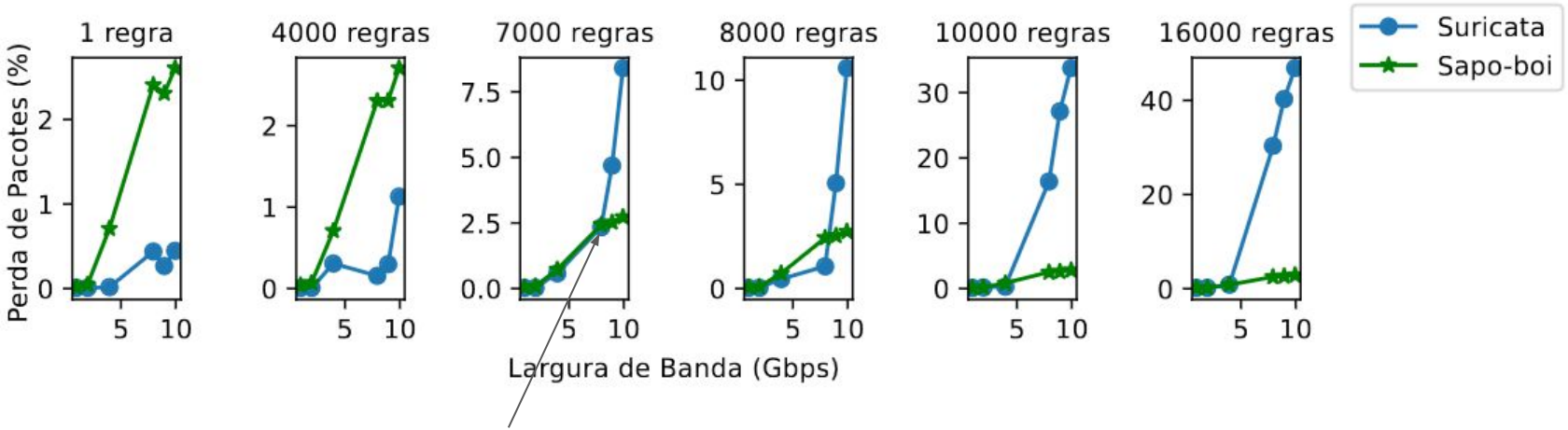
Avaliação - Pacotes Analisados

- Como o número de regras carregadas afeta as soluções?



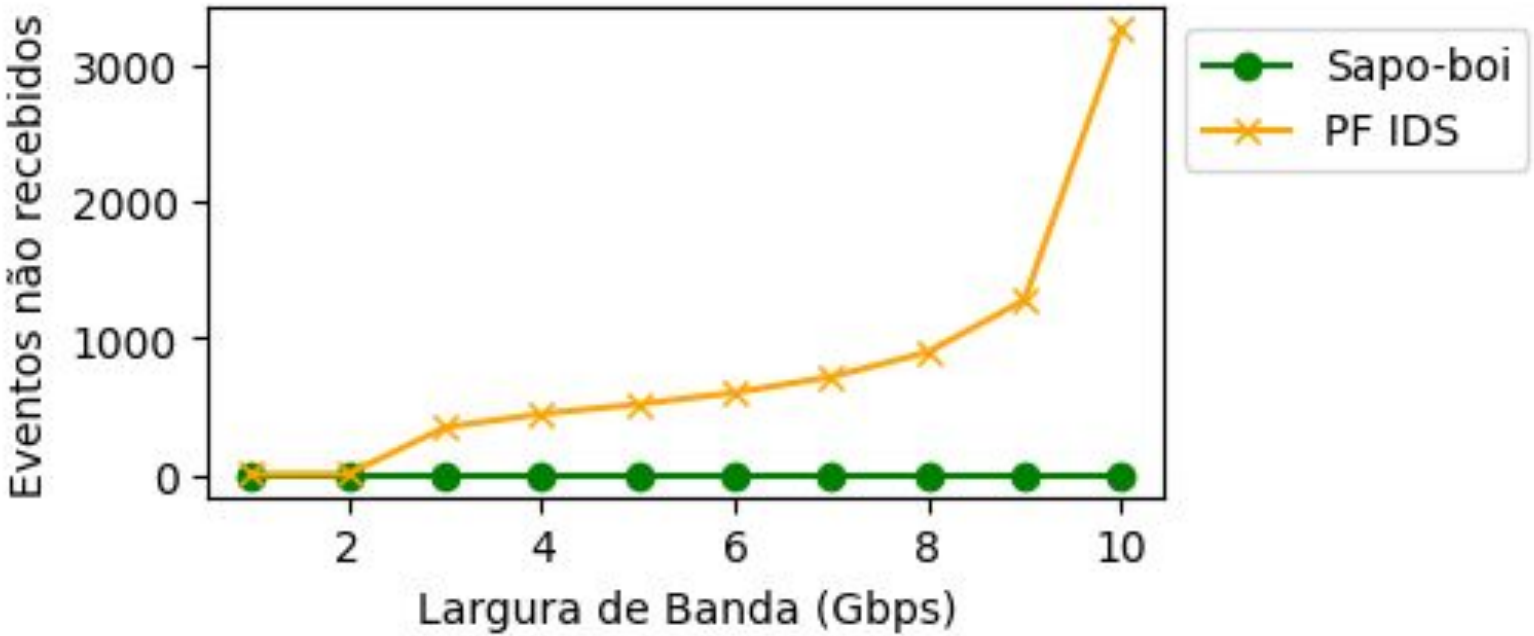
Avaliação - Pacotes Analisados

- Como o número de regras carregadas afeta as soluções?

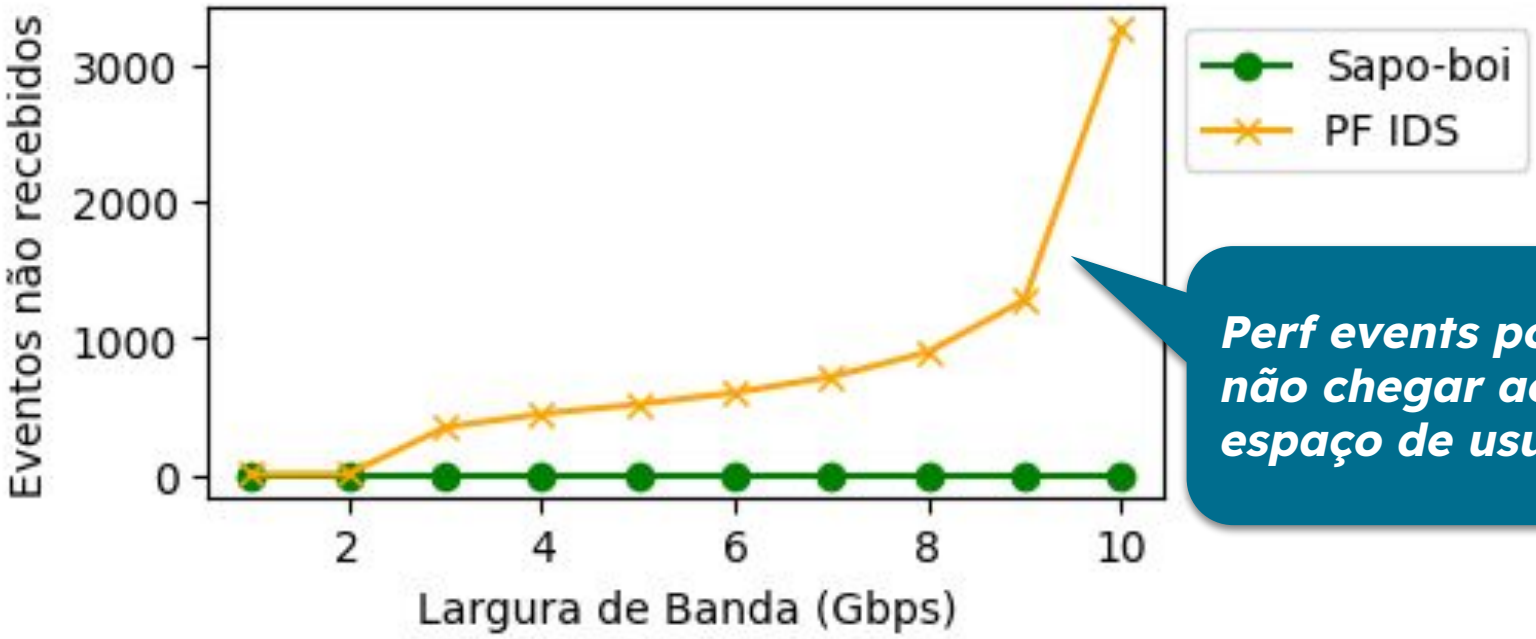


Ponto de Inflexão!

Avaliação - Passagem de pacotes suspeitos



Avaliação - Passagem de pacotes suspeitos



Considerações finais

- Influência da quantidade de regras carregadas
  - *Maior em soluções inteiramente em usuário*
- Influência da largura de banda
  - *Notável em todas as soluções. Maior impacto nas soluções de usuário*
- SAPO-BOI supera PF IDS na capacidade de gerar potenciais alertas

Trabalhos futuros

- Estudar o comportamento das soluções com bases de regras e de ataques mais realistas
- Avaliação da quantidade de alertas gerados pelas soluções.

Agradecimentos

- Os autores agradecem à CAPES e BluePex pelo financiamento deste trabalho

Obrigado!

- Raphael Kaviak Machnicki
- rkmachnicki@inf.ufpr.br