IX FÓRUM REGIONAL
Incentivando o diálogo sobre os Pontos de Troca de Tráfego Internet
14 de Agosto de 2026
Edição Nordeste - Campina Grande/PB

ATAQUES INTERNOS EM ISPs

Como detectar e combater essa ameaça?

Neste exato momento, as redes que vocês gerenciam podem estar atacando outras empresas e vocês nem sabem disso.

Tales Rodarte • YouISP - You Soluções

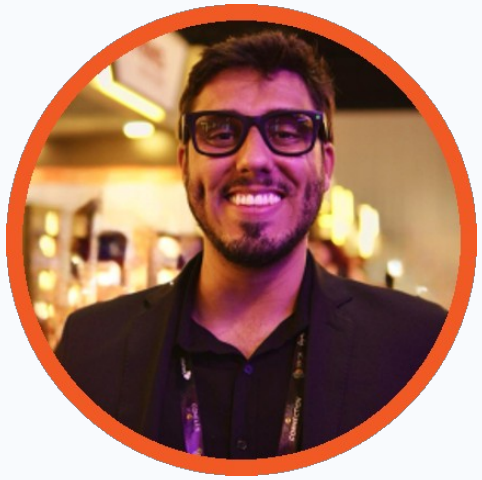
14 de Agosto de 2026 • Campina Grande/PB

Baixe os slides

youisp.com.br/tales-rodarte-ataques-ddos-internos.pdf

Quem sou eu

Uma visão rápida para contextualizar a experiência e as empresas que represento.



Tales Rodarte

Profissional de redes, segurança e telecomunicações, com atuação em ISPs, sistemas autônomos, DDoS, BGP, CGNAT, observabilidade e automação.

YouISP

Engenharia de redes, servidores e segurança para sistemas autônomos.

Grupo WE DEV

Software para ISPs, automações, Cloud, mitigação DDoS e venda de equipamentos.

Antes de começar: quem está na sala?

A mesma ameaça aparece de formas diferentes para quem opera rede e para quem depende dela.

Quem trabalha diretamente com provedor de internet?

Quem vem de outros segmentos, mas depende da Internet para operar?

O ataque que afeta uma empresa externa pode estar sendo gerado dentro da base residencial de um ISP , muitas vezes por dispositivos infectados que continuam funcionando normalmente.

1 Panorama

por que o problema cresceu

2 Caso real

sintomas em ISP regional

3 Detecção

CGNAT, flow e captura

4 Resposta

FlowSpec, filtros e prevenção

Brasil conectado: mais escala, mais exposição

O mesmo crescimento que impulsiona o mercado também amplia a superfície para ataques e abusos.

18,8 mil
operadoras SCM registradas em 2025
base Anatel consolidada no mercado

19,5 mil
provedores outorgados em 2026
após regularização do setor

76 mi
domicílios com Internet em 2025
95% dos lares brasileiros

502 mi
dispositivos digitais em uso em 2025
2,4 por habitante

470.677
ataques DDoS contra o Brasil
jul a dez de 2025

17.527
ataques em apenas 6 dias
contra o Brasil em 2026

25 mi
dispositivos em residências brasileiras
usados recorrentemente em DDoS

78%
dos ataques terminam
em até 5 minutos

52%
atingem múltiplos hosts
simultaneamente

Mais assinantes, mais dispositivos e mais provedores significam mais oportunidades para o atacante escalar sem chamar atenção.

Fontes: Anatel/TeleTime, IBGE PNAD TIC 2025, FGVcia 2025, NETSCOUT ATLAS, A10 Networks, Nokia Deepfield e TeleSíntese.

O DDoS mudou de comportamento

Hit-and-run continua existindo, mas agora divide espaço com automação, carpet bombing e multivetor.

ANTES: hit-and-run

- picos rápidos e concentrados
- alvo único ou mais previsível
- resposta humana ainda chegava a tempo em muitos casos

AGORA: automação + escala

- ataques curtos demais para resposta manual
- múltiplos hosts e múltiplos vetores
- ISPs menores passam a aparecer no caminho do ataque

O novo mínimo: baseline + correlação + bloqueio local.

Fonte: Nokia Deepfield , "DDoS in 2025: The year automation took the wheel".

O problema não está só “na Internet”

Ele pode estar no roteador, na TV Box, no aplicativo suspeito ou no dispositivo IoT da casa do assinante.

TVs Android / WebOS

apps de origem duvidosa e TV gratuita

TV Box e projetores

software sem atualização e pouca rastreabilidade

Câmeras, lâmpadas e IoT

firmware antigo, senha padrão e C&C

Proxy residencial

terceiro usando IP residencial para fraudes

O dispositivo infectado não precisa parar de funcionar para atacar alguém.

Caso real: ISP regional em São Paulo

Mais de 10 mil assinantes, CPEs variadas e sintomas aparecendo antes do diagnóstico.

Reclamações acima do normal

lentidão, quedas rápidas, instabilidade percebida

CGNAT fora do padrão

sessões, portas e conexões acima do esperado

Upload excessivo nos links

picos em horários variados, sem padrão comercial claro

Dispositivos heterogêneos

ONUs, roteadores e equipamentos residenciais variados

Hipótese que abriu a investigação: o problema não estava apenas no backbone; havia tráfego malicioso saindo de assinantes.

Stack de investigação: coleta, monitoramento e resposta

Nenhuma ferramenta resolve sozinha. O resultado vem da combinação de telemetria, baseline, correlação e ação.

Coletar

NETFLOW/IPFIX
sFlow
Port mirror
tcpdump
RADIUS Accounting

Monitorar

SNMP: Zabbix, LibreNMS, Prometheus
Grafana
Borda, CGNAT e firewall
Interfaces: bps e pps
Chamados no suporte
Relatórios RADIUS/ERP

Detectar

Wanguard Console
RRFLOW
GWD ODIN
FastNetMon
sFlow-RT
nfdump

Correlacionar

LLMs para organizar evidências
RADIUS/ERP + CGNAT
MACs internos via TR-069
Modelo de CPE e dispositivo
Horário, decoder e destino

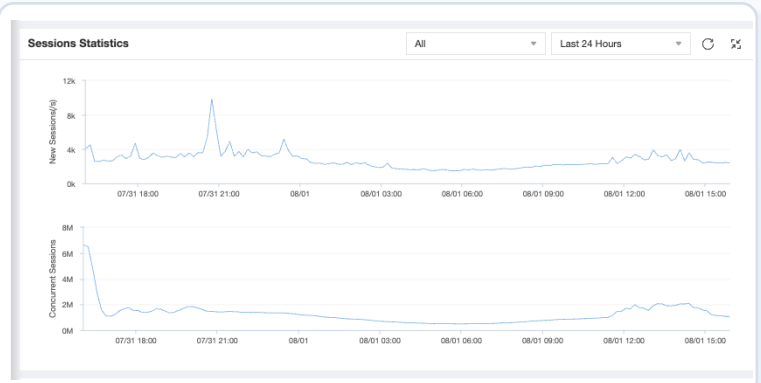
Mitigar

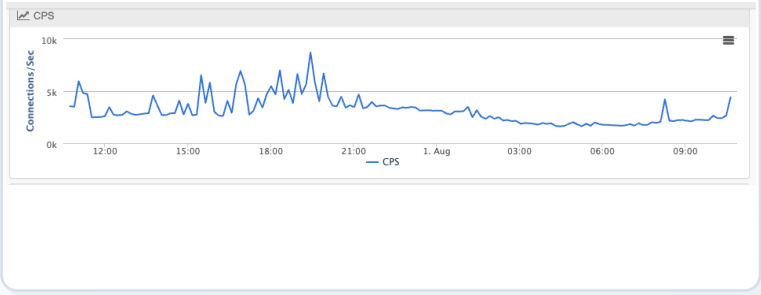
Wanguard Filter
FlowSpec
ExaBGP e GoBGP
Listas de reputação e C&C
Rate-limit: sessões, CPS e portas
NGFW e ACLs

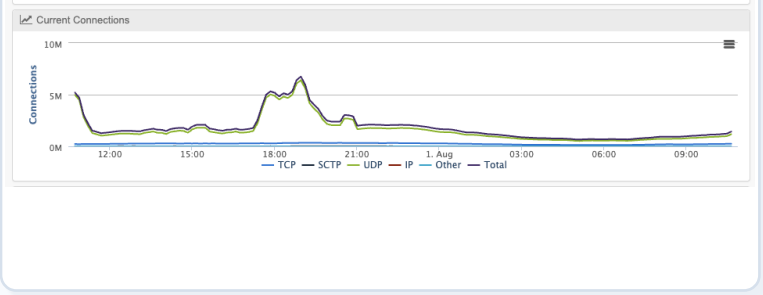
O ponto de virada não foi uma ferramenta específica. Foi cruzar sinais fracos até formar evidência operacional.

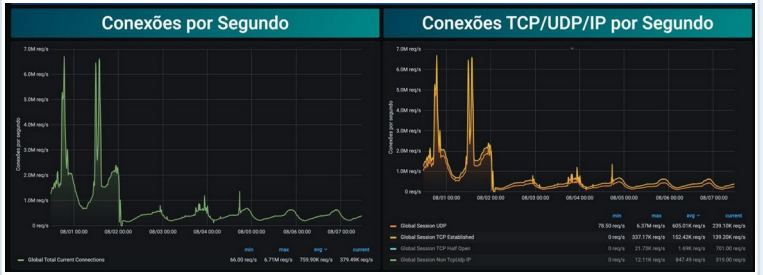
Análise 1: CGNAT, sessões e picos

A primeira pista operacional aparece quando sessões, portas e conexões deixam de seguir o comportamento esperado.



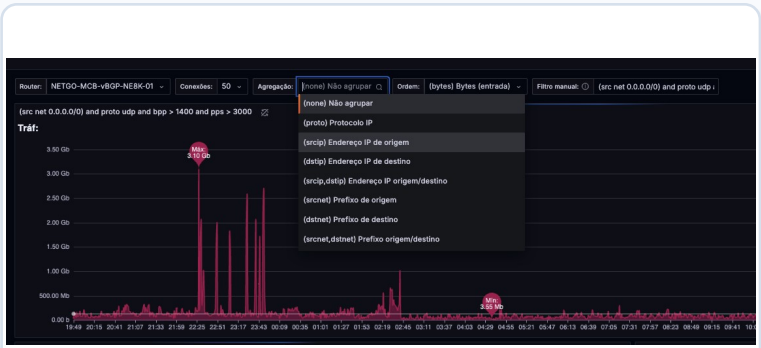


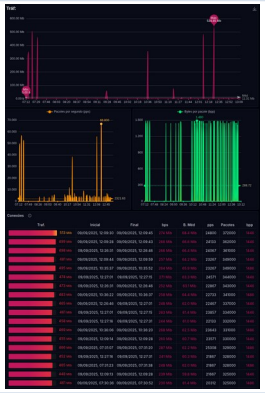


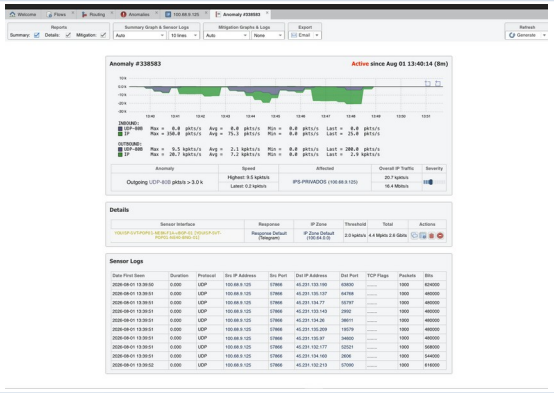


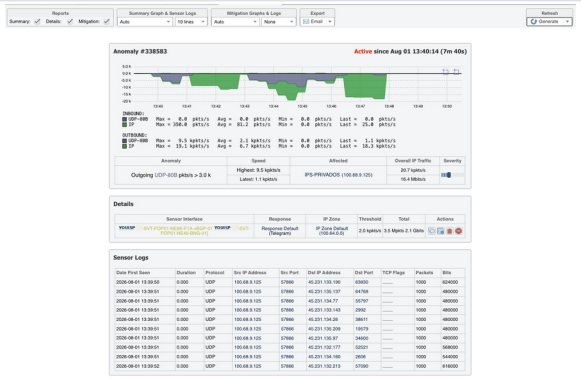
Análise 2: visibilidade por flow e ferramentas especializadas

Flow deixa de ser “relatório bonito” e vira ferramenta de triagem operacional.



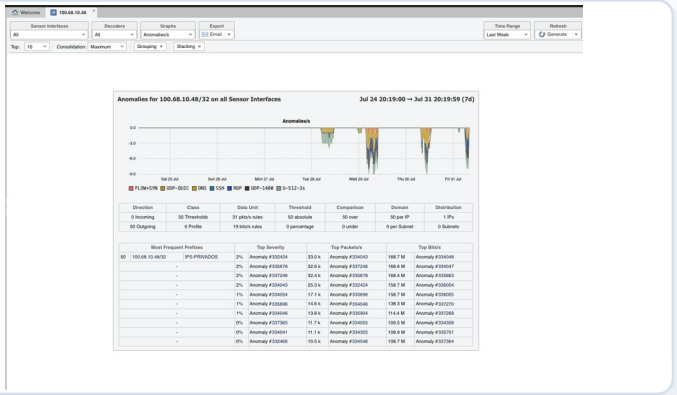


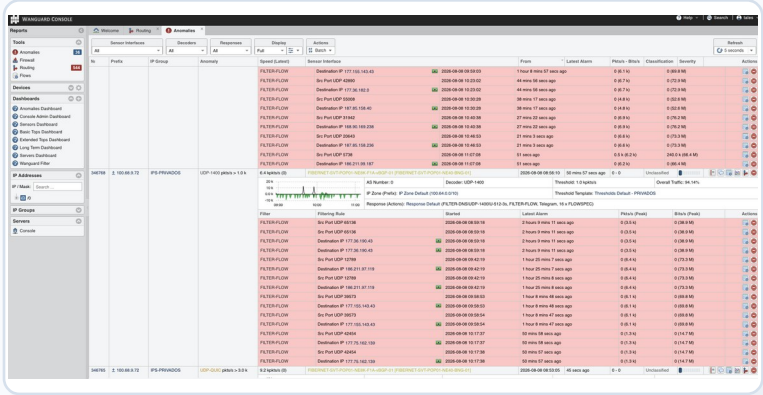


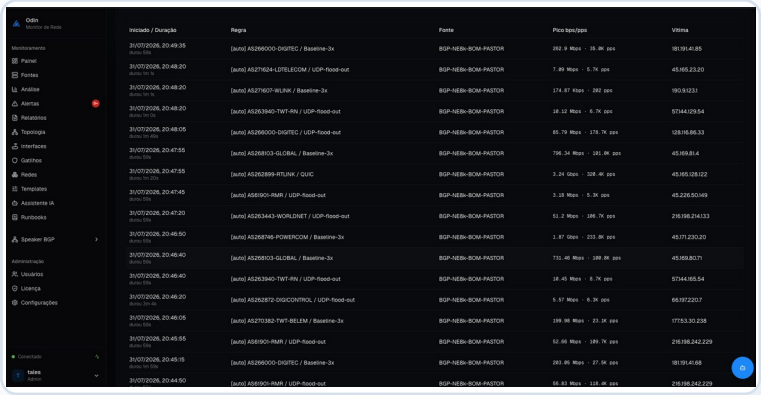


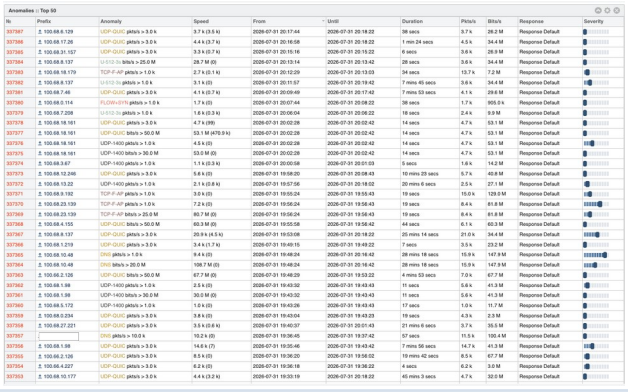
Análise 3: incidentes, anomalias e ranking

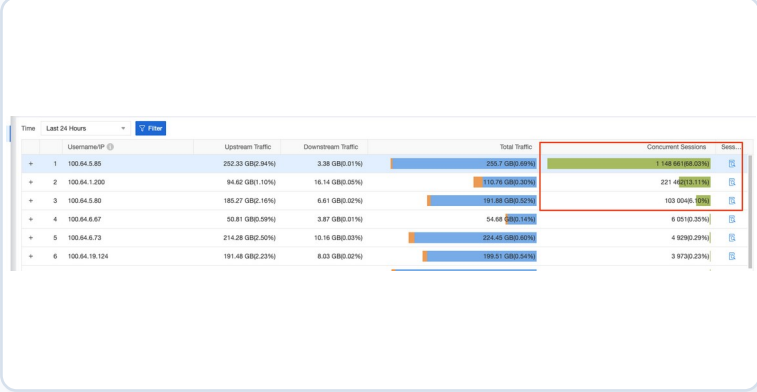
Quando o incidente vira recorrente, o importante é transformar evento em prioridade de ação.





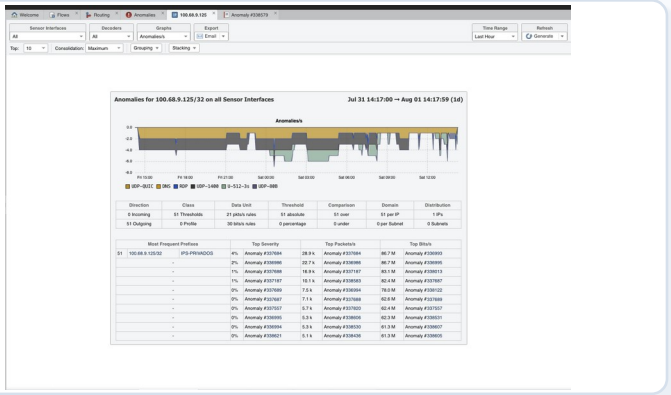


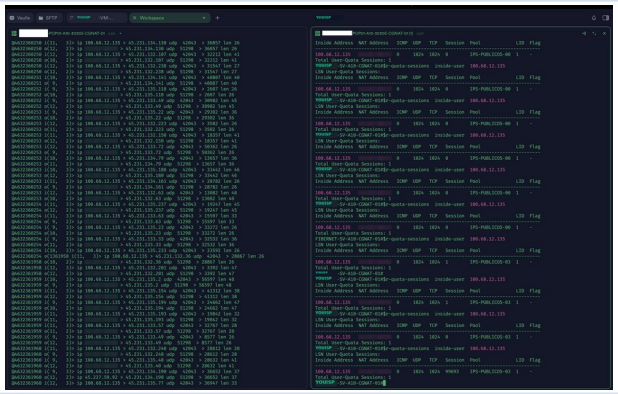


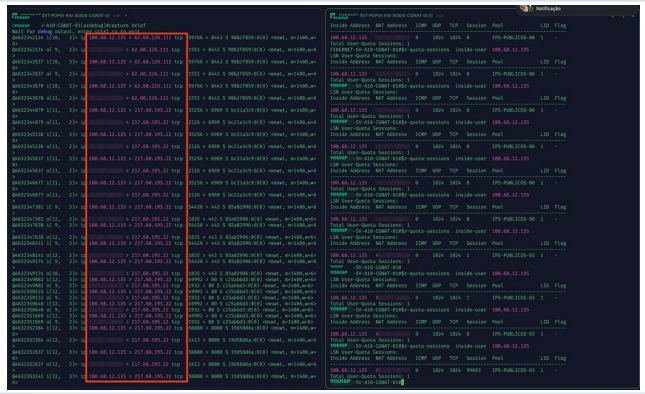


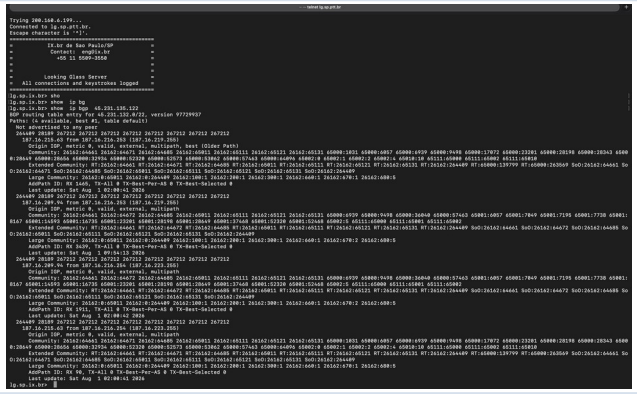
Análise 4: captura de pacotes no A10

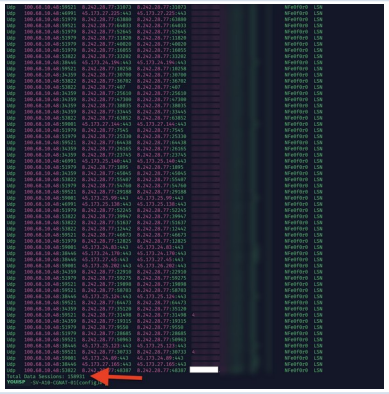
A captura confirma padrão de ataque, destinos recorrentes e indícios de controle da botnet.

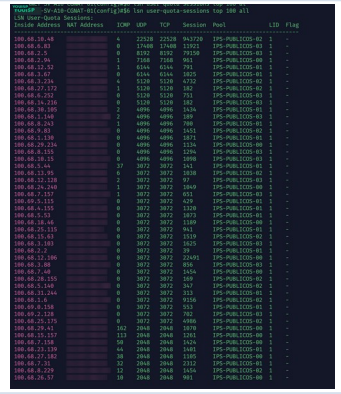






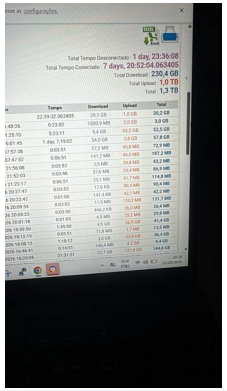


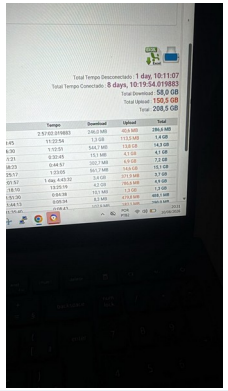


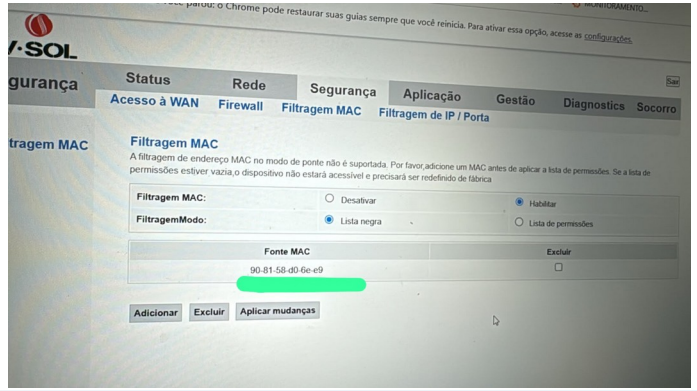


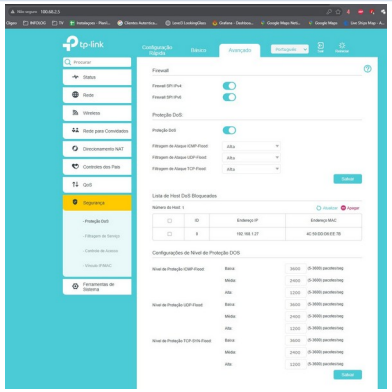
Análise 5: usuários, portas e dispositivos residenciais

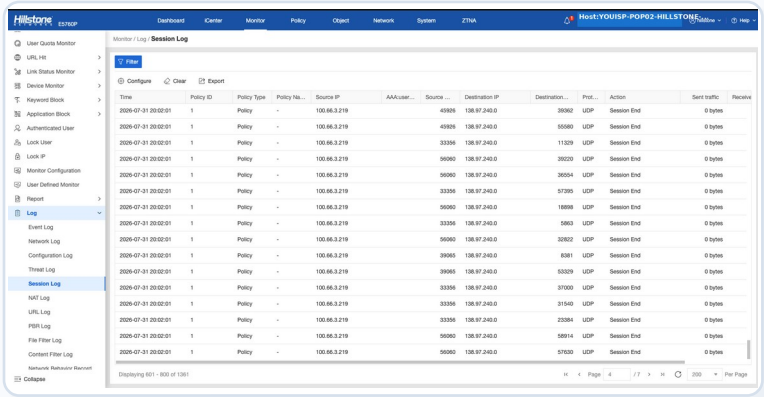
A correlação com o assinante ajuda a sair do “ataque genérico” para ações concretas.

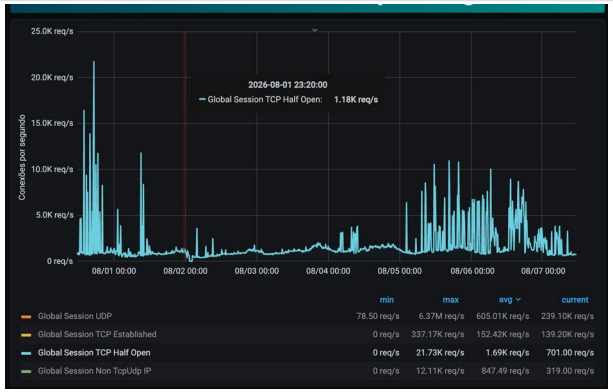






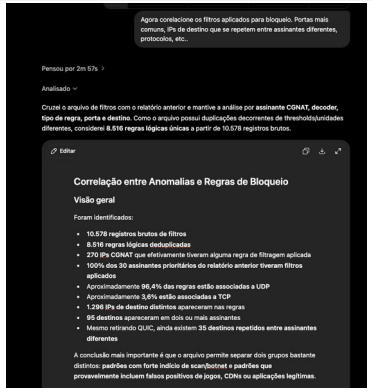


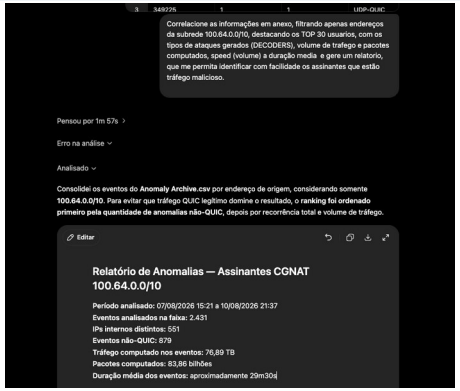


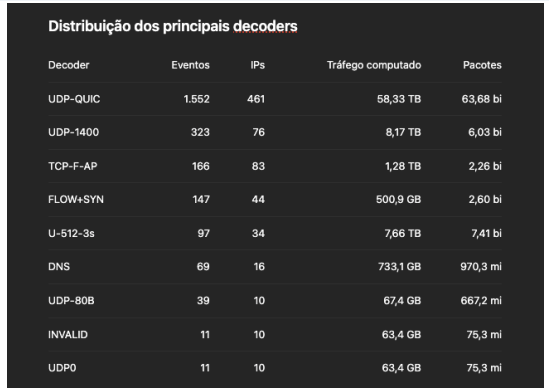


Análise 6: correlação, IA e listas de ameaça

LLMs ajudam a organizar evidências; TR-069, RADIUS, CGNAT e flows ajudam a ligar o evento ao assinante e ao dispositivo.

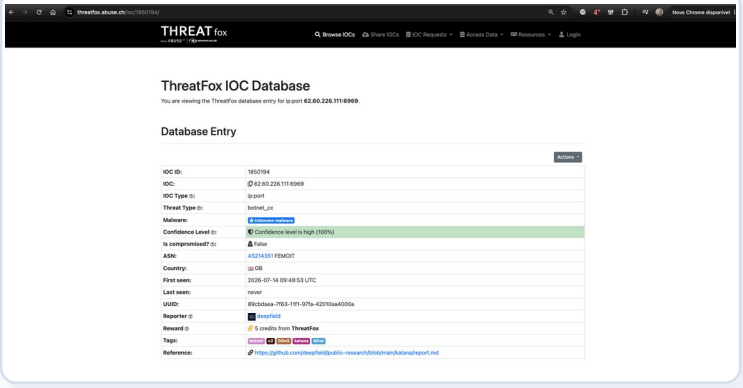






Distribuição dos principais decoders

Decoder	Eventos	IPs	Tráfego computado	Pacotes
UDP-QUIC	1.552	461	58,33 TB	63,68 bi
UDP-1400	323	76	8,17 TB	6,03 bi
TCP-F-AP	166	83	1,28 TB	2,26 bi
FLOW+SYN	147	44	500,9 GB	2,60 bi
U-512-3s	97	34	7,66 TB	7,41 bi
DNS	69	16	733,1 GB	970,3 mi
UDP-80B	39	10	67,4 GB	667,2 mi
INVALID	11	10	63,4 GB	75,3 mi
UDP0	11	10	63,4 GB	75,3 mi



5. Portas UDP mais recorrentes

Porta	Assinantes	Regras	Observação
53	6	50	DNS — investigar abuso
65535	5	58	QUIC/UDP-1400; comportamento incomum
1194	5	31	Porta padrão de OpenVPN; validar aplicação
1701	5	19	Porta associada a L2TP; revisar contexto
25565	2	6	Recorrente em UDP
22	2	5	Uso UDP incomum
7443	2	4	UDP-1400

Existe um padrão muito claro em cinco dos clientes mais críticos:

`100.68.0.23`
`100.68.12.56`
`100.68.6.0`
`100.68.2.188`
`100.68.13.178`

Eles compartilham várias ocorrências para:

UDP/65535, UDP/1194 e UDP/1701

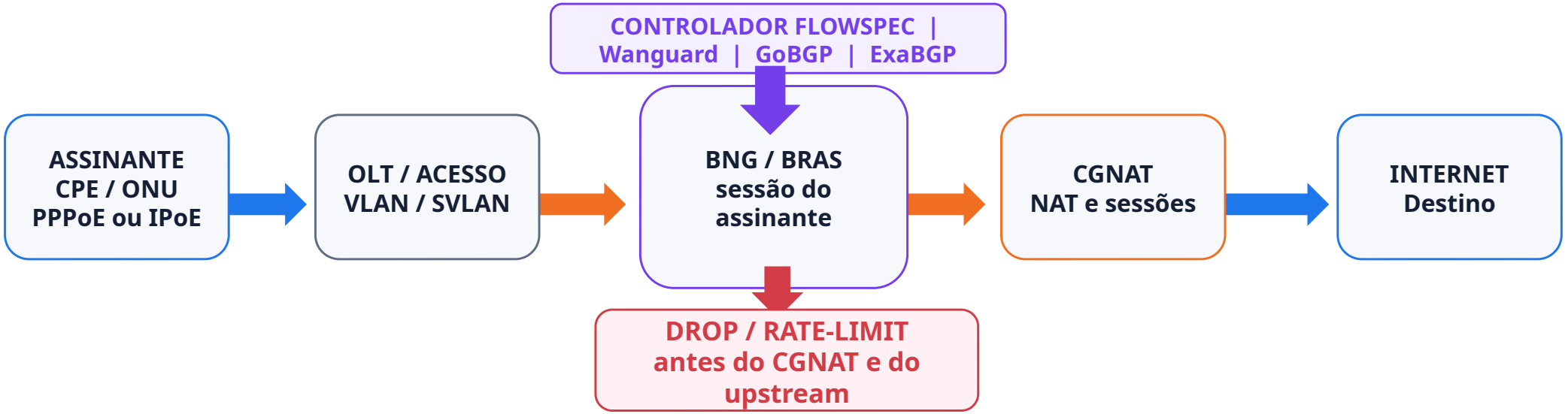
Entretanto, como alguns desses mesmos assinantes também apresentam tráfego para Roblox e outros serviços de jogos, esse grupo UDP deve ser tratado com menor confiança que o padrão TCP/23.

Regra prática

IA não decide sozinha. Ela acelera análise, cruza padrões e ajuda a transformar logs, flows, MACs e decoders em hipóteses de mitigação.

FlowSpec no concentrador: bloquear perto do assinante

Quando o BNG aplica a regra no ponto de autenticação, o tráfego malicioso pode ser contido antes do CGNAT e do upstream.



VALIDAÇÃO NO BNG

Nem todo BNG permite o bloqueio em interfaces virtuais (PPPoE, IPoE, L2TP, IRB, Virtual-Ethernet etc.). Valide a contabilização das regras e a efetividade.
Alguns requerem atualização e mudanças de parâmetros no slot/chassi ou placa especial de serviço.

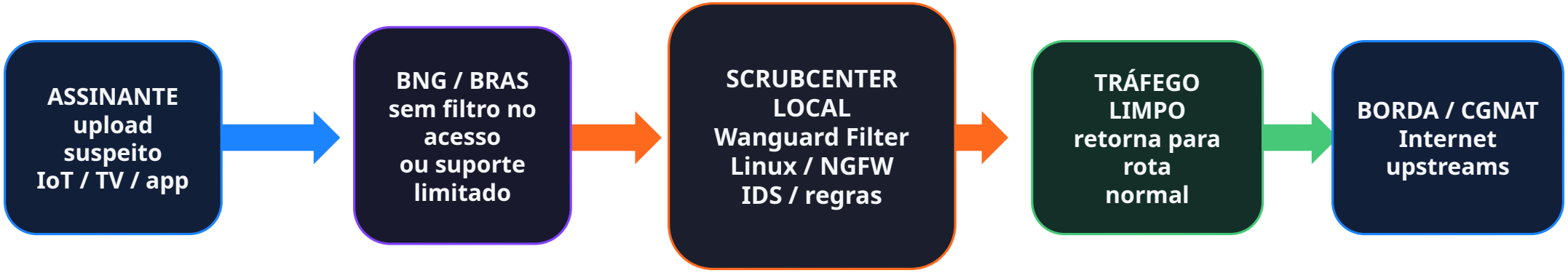
CHEQUE A DOCUMENTAÇÃO

Huawei NE40 / NE8000: valide versão e suporte.
No cenário apresentado, considere R24 ou superior para esse tipo de aplicação.
A posição de aplicação da regra varia entre fabricantes e plataformas.

Quando o concentrador não filtra: desviar upload para scrubcenter local

O tráfego de saída pode ser redirecionado para inspeção e limpeza antes de chegar ao CGNAT, borda ou trânsito.

UPLOAD → limpeza local → retorno limpo



Como fazer o desvio

- policy route, VRF, next-hop ou túnel local
- desvio seletivo do upload suspeito
- mantém o tráfego comum na rota normal

O que aplicar no scrubcenter

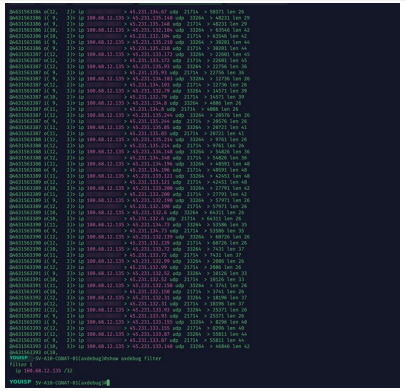
- Wanguard Filter, ACLs, NGFW ou scripts locais
- FlowSpec, listas e filtros por decoder
- rate-limit por sessão, CPS, portas e volume

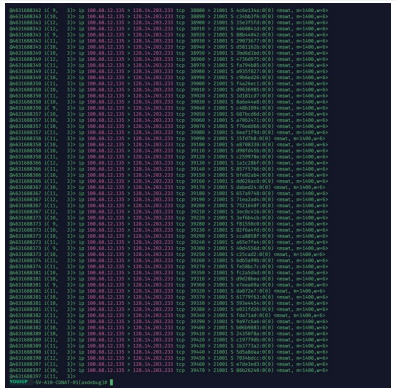
Quando usar

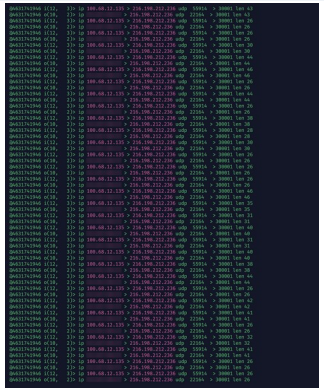
- concentrador não suporta FlowSpec no acesso
- precisa proteger CGNAT e uplinks rapidamente
- quer reduzir tráfego ruim antes de sair da rede

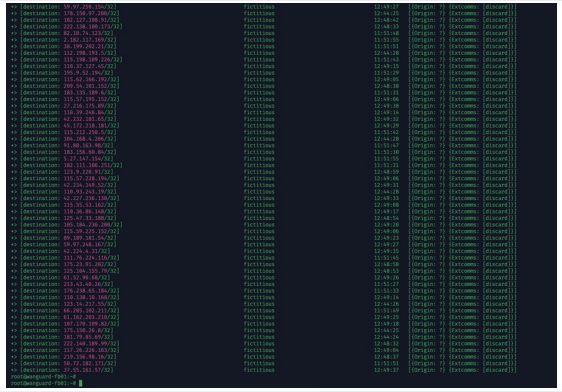
Mitigação: bloquear antes de sair da rede

Wanguard Filter, FlowSpec, ExaBGP, GoBGP, listas e rate-limit reduzem o volume que chega ao alvo e protegem o CGNAT.









Prefix	BGP Connector	Role	Status	Originator	From	Until	Flowspec	Comments	Actions
100.68.2.128/32	FLOWSPEC-GOBGP	Mitigation	✓	Anomaly #338372 (Filtering Rule #407625)	2026-08-01 10:37:00	∞	source 100.68.2.128/32; destination 109.241.200.48/32; port 53; discard;	-	
			✓	Anomaly #338371 (Filtering Rule #407626)	2026-08-01 10:37:05	∞	source 100.68.2.128/32; destination 109.241.200.48/32; port 53; discard;	-	
100.68.11.133/32	FLOWSPEC-GOBGP	Mitigation	✓	Anomaly #338325 (Filtering Rule #407619)	2026-08-01 10:17:20	∞	source 100.68.11.133/32; destination 120.48.88.116/32; port 53; discard;	-	
			✓	Anomaly #338324 (Filtering Rule #407620)	2026-08-01 10:17:31	∞	source 100.68.11.133/32; destination 120.48.88.116/32; port 53; discard;	-	
			✓	Anomaly #338325 (Filtering Rule #407621)	2026-08-01 10:31:19	∞	source 100.68.11.133/32; destination 145.239.236.30/32; port 53; discard;	-	
			✓	Anomaly #338324 (Filtering Rule #407622)	2026-08-01 10:31:30	∞	source 100.68.11.133/32; destination 145.239.236.30/32; port 53; discard;	-	
			✓	Anomaly #338325 (Filtering Rule #407623)	2026-08-01 10:32:19	∞	source 100.68.11.133/32; destination 37.225.90.116/32; port 53; discard;	-	
			✓	Anomaly #338324 (Filtering Rule #407624)	2026-08-01 10:32:30	∞	source 100.68.11.133/32; destination 37.225.90.116/32; port 53; discard;	-	
			✓	Anomaly #338325 (Filtering Rule #407627)	2026-08-01 10:37:59	∞	source 100.68.11.133/32; destination 193.192.177.150/32; port 53; discard;	-	
			✓	Anomaly #338324 (Filtering Rule #407628)	2026-08-01 10:38:05	∞	source 100.68.11.133/32; destination 193.192.177.150/32; port 53; discard;	-	

Ciclo de resposta

Detectar e correlacionar
Criar regra local
Anunciar via FlowSpec
Aplicar Filter, ACL ou NGFW
Rate-limit de sessões, CPS e portas
Medir queda no tráfego e nas sessões

Fechamento: o dever de casa do ISP

Se cada provedor reduz o tráfego malicioso que nasce dentro da sua rede, toda a Internet fica mais simples de proteger.

1 Enxergar

flow, sessões, portas, upload, bps, pps e chamados

2 Correlacionar

assinante, destino, decoder, MAC via TR-069 e horário

3 Conter

FlowSpec, Filter, ExaBGP, GoBGP, NGFW, ACL e rate-limit

4 Antecipar

listas C&C, reputação, alertas, automação e revisão de CPEs

O ISP que enxerga e trata a própria rede deixa de ser apenas vítima. Passa a reduzir o problema antes que ele ganhe escala.

Obrigado!

DÚVIDAS?

Ou você ainda acha que os TVBOX estão somente reproduzindo canais?

ISP: "Meu link está estranho... será que é o upstream?"

TV Box: "Relaxa... estou só fazendo um uploadzinho de 300Mbps."

"Só um tráfego normal"

ALVO NA INTERNET

Moral da história:
Se você não monitora sua rede, alguém pode estar controlando os dispositivos dos seus clientes e transformando seus recursos em produto.

Obrigado!

Fico à disposição para dúvidas, networking e continuidade da conversa.

Tales Rodarte

trodarte@you.solutions | trodarte@grupowedev.com.br

Fone: +55 35 99869-6077

Redes sociais e Telegram: @talesrodarte

You Soluções | Grupo We DEV

https://youisp.com.br | https://grupowedev.com.br

WhatsApp

Escaneie para falar comigo