



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

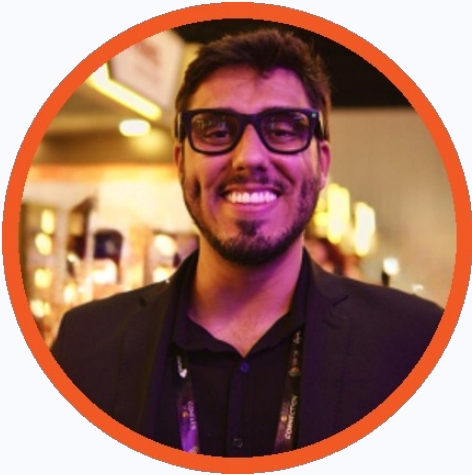


Baixe os slides

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

2/5



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

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.

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

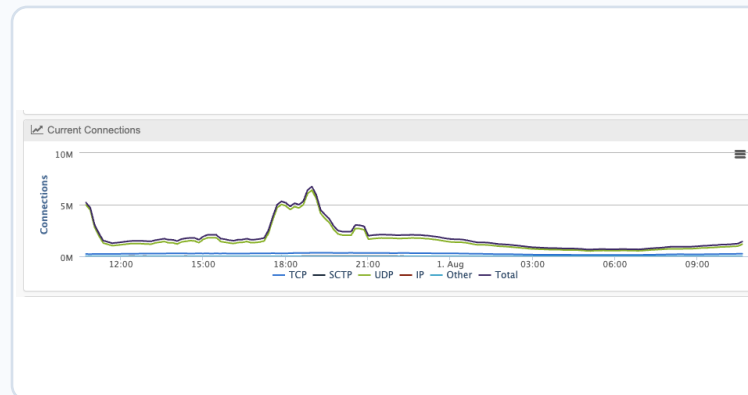
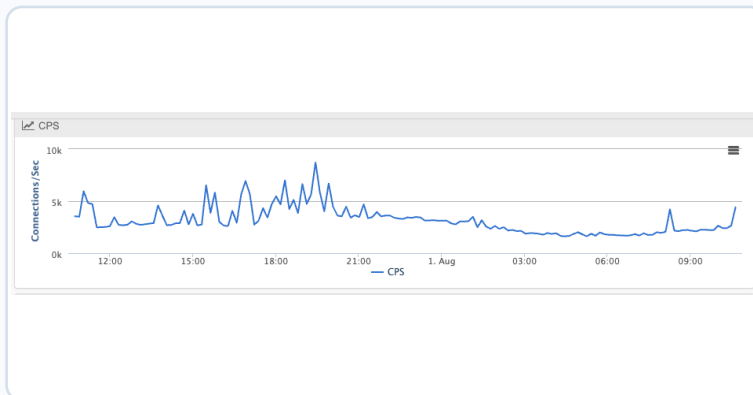
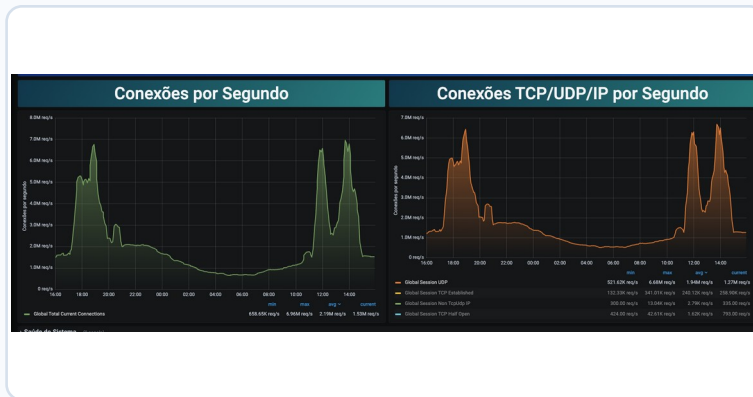
Mitigar

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.

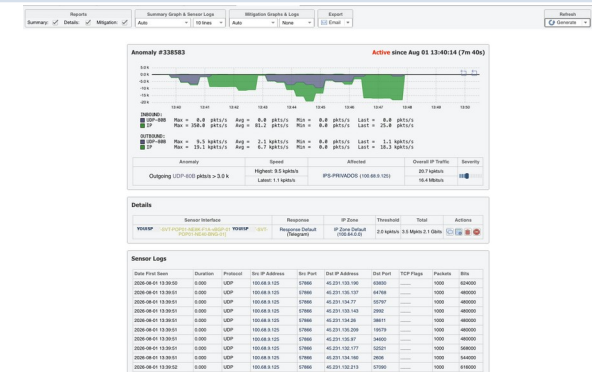
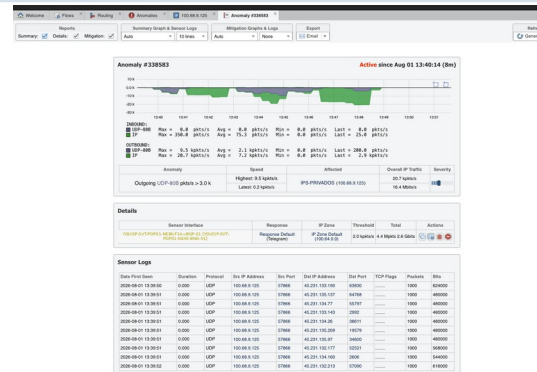
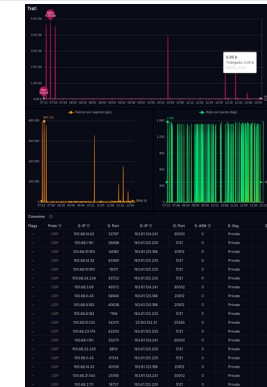
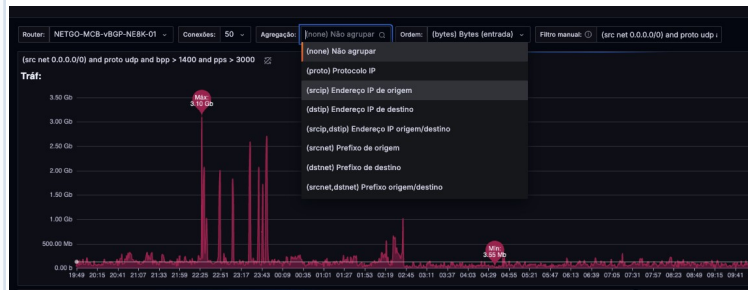
Análise 1: CGNAT, sessões e picos

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



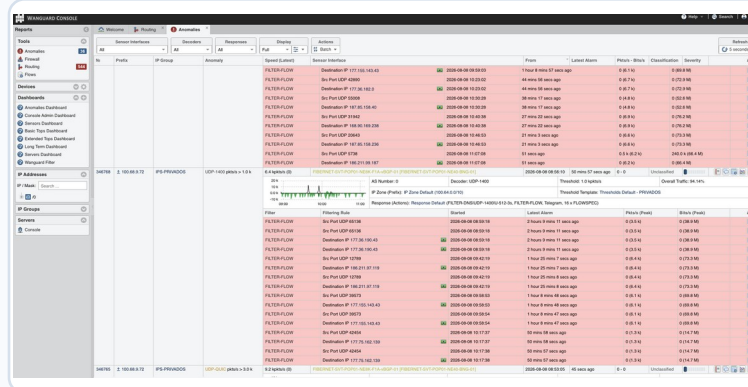
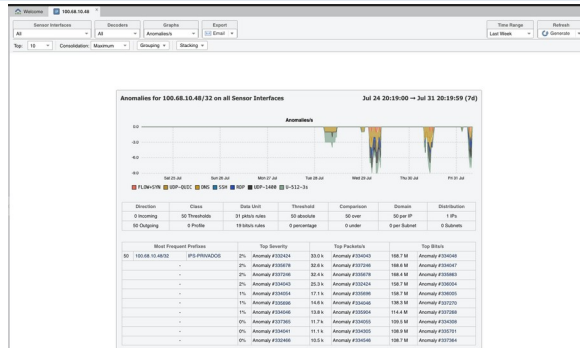
Análise 2: visibilidade por flow e ferramentas especializadas

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



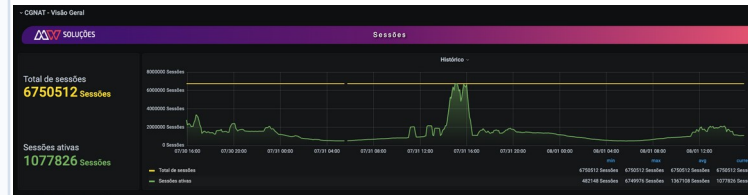
Análise 3: incidentes, anomalias e ranking

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



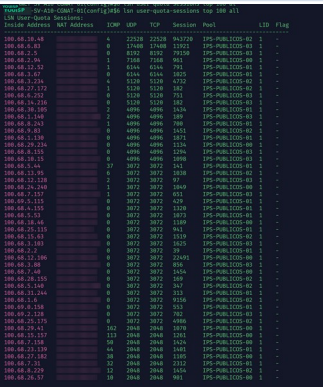
Regras	Regra	Faixa	Plano (bytes)	Uptime
3/20/2026, 20:49:35	[name] AS26000-DIGITEC / Baseline-3x	BGP-NEB-BGM-PASTOR	162.8 Mbit - 16.8M pps	18391.43s
3/20/2026, 20:49:20	[name] AS27024-LISTECOM / UGP-Road-out	BGP-NEB-BGM-PASTOR	7.89 Mbit - 5.7M pps	45195.232s
3/20/2026, 20:48:20	[name] AS27007-WEBA / Baseline-3x	BGP-NEB-BGM-PASTOR	174.87 Mbit - 282 pps	59019.02s
3/20/2026, 20:48:20	[name] AS26340-TAT-AM / UGP-Road-out	BGP-NEB-BGM-PASTOR	18.13 Mbit - 6.7M pps	87648.0934s
3/20/2026, 20:48:05	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	65.19 Mbit - 171.7M pps	12816.8633s
3/20/2026, 20:47:55	[name] AS26000-DIGITEC / Baseline-3x	BGP-NEB-BGM-PASTOR	706.34 Mbit - 321.8M pps	45189.81s
3/20/2026, 20:47:55	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	1.34 Mbit - 108.4M pps	45195.1282s
3/20/2026, 20:47:45	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	1.38 Mbit - 5.3M pps	45226.5046s
3/20/2026, 20:47:20	[name] AS26340-WORLDNET / UGP-Road-out	BGP-NEB-BGM-PASTOR	12.2 Mbit - 186.7M pps	21616.24133s
3/20/2026, 20:46:50	[name] AS26000-DIGITEC / Baseline-3x	BGP-NEB-BGM-PASTOR	1.87 Mbit - 235.0M pps	45171.2320s
3/20/2026, 20:46:40	[name] AS26000-DIGITEC / Baseline-3x	BGP-NEB-BGM-PASTOR	172.46 Mbit - 199.8M pps	45189.8071s
3/20/2026, 20:46:40	[name] AS26340-TAT-AM / UGP-Road-out	BGP-NEB-BGM-PASTOR	28.45 Mbit - 6.7M pps	87648.0934s
3/20/2026, 20:46:20	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	1.97 Mbit - 6.7M pps	45177.2207s
3/20/2026, 20:46:05	[name] AS27024-TAT-AM / Baseline-3x	BGP-NEB-BGM-PASTOR	198.98 Mbit - 31.7M pps	17733.3238s
3/20/2026, 20:45:55	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	12.66 Mbit - 181.7M pps	21616.24133s
3/20/2026, 20:45:55	[name] AS26000-DIGITEC / Baseline-3x	BGP-NEB-BGM-PASTOR	181.65 Mbit - 27.1M pps	45189.81s
3/20/2026, 20:44:50	[name] AS26000-DIGITEC / UGP-Road-out	BGP-NEB-BGM-PASTOR	18.83 Mbit - 118.4M pps	21616.24133s

Assomias - Top 10	Assomias	Spikes	From	To	Duration	Plano	Stress	Response
3/20/26	100.68.1.129	100.68.1.129	2026-07-31 20:17:44	2026-07-31 20:18:02	18 secs	3.7A	28.2M	Response Default
3/20/26	100.68.1.226	100.68.1.226	2026-07-31 20:18:08	2026-07-31 20:18:22	14 secs	4.3A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	38.9M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default
3/20/26	100.68.1.137	100.68.1.137	2026-07-31 20:18:16	2026-07-31 20:18:22	6 secs	5.6A	34.4M	Response Default



Time	Last 24 Hours	Y Axis	Username/IP	Upstream Traffic	Downstream Traffic	Total Traffic	Concurrent Sessions	Score
1	100.68.1.80	252.33 GB (2.4%)	3.38 GB (0.1%)	255.71 GB (2.5%)	1.44 GB (1.4%)	221.48 (11.1%)	100.00 (0%)	100.00 (0%)
2	100.68.1.200	84.62 GB (1.0%)	16.14 GB (0.2%)	100.76 GB (1.2%)	100.76 GB (1.2%)	4.9360 (2.9%)	100.00 (0%)	100.00 (0%)
3	100.68.1.80	185.27 GB (1.6%)	6.61 GB (0.2%)	191.88 GB (2.2%)	191.88 GB (2.2%)	4.9360 (2.9%)	100.00 (0%)	100.00 (0%)
4	100.68.1.87	50.81 GB (0.5%)	3.87 GB (0.1%)	54.68 GB (0.6%)	54.68 GB (0.6%)	6.0510 (3.0%)	100.00 (0%)	100.00 (0%)
5	100.68.1.73	214.28 GB (2.0%)	10.16 GB (0.3%)	224.44 GB (2.3%)	224.44 GB (2.3%)	4.9360 (2.9%)	100.00 (0%)	100.00 (0%)
6	100.68.1.124	191.48 GB (2.3%)	8.03 GB (0.2%)	199.51 GB (2.5%)	199.51 GB (2.5%)	3.9730 (2.3%)	100.00 (0%)	100.00 (0%)

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



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.

Agora correlacione os filtros aplicados para bloqueio. Portas mais comuns, IPs de destino que se repetem entre assinantes diferentes, protocolos, etc...

Pensou por 2m 57s

Analisado

Cruze o arquivo de filtros com o relatório anterior e mantenha a análise por assinante CGNAT, decoder, tipo de regra, porta e destino. Como a análise possui múltiplas decodificações de threatfox/entidades diferentes, considere 8.519 regras lógicas únicas a partir de 10.579 registros brutos.

Correlação entre Anomalias e Regras de Bloqueio

Visão geral

Filtros identificados:

- 10.579 registros brutos de filtros
- 8.519 regras lógicas deduplicadas
- 270 IPs CGNAT que efetivamente tiveram alguma regra de filtragem aplicada
- 100% dos 10 assinantes prioritários do relatório anterior tiveram filtros aplicados
- Aproximadamente 95,4% das regras estão associadas a UDP
- Aproximadamente 8,6% estão associadas a TCP
- 1.298 IPs de destino distintos apareceram nas regras
- 95 destinos apareceram em dois ou mais assinantes
- Mais de 20 regras repetidas entre assinantes diferentes

A conclusão mais importante é que o arquivo permite separar dois grupos bastante distintos: padrões com forte indicio de scan/bruteforce e padrões que provavelmente incluem regras positivas de jogos, CDNs ou aplicações legítimas.

Correlacione as informações em anexo, filtrando apenas endereços da subrede 100.64.0.0/10, destacando os TOP 30 usuários, com os tipos de ataques gerados (DECODERS), volume de tráfego e pacotes computados, speed (volume) e duração média e gere um relatório, que me permita identificar com facilidade os assinantes que estão tráfego malicioso.

Pensou por 1m 57s

Erro na análise

Analisado

Consolide os eventos do Anomaly Archive.csv por endereço de origem, considerando somente 100.64.0.0/10. Para evitar que tráfego QUIC legítimo distorça o resultado, o ranking foi ordenado primeiro pela quantidade de anomalias não-QUIC, depois por recorrência total e volume de tráfego.

Relatório de Anomalias – Assinantes CGNAT 100.64.0.0/10

Período analisado: 07/08/2025 15:21 a 10/08/2025 21:37

Eventos analisados na faixa: 2.431

IPs internos distintos: 561

Eventos não-QUIC: 879

Tráfego computado nos eventos: 76,89 TB

Pacotes computados: 83,86 bilhões

Duração média dos eventos: aproximadamente 29m30s

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	89	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

THREATfox

ThreatFox IOC Database

You are viewing the ThreatFox database entry for ipport 82.69.226.111:8080.

Database Entry

IOC ID: 180294

IOC: 82.69.226.111:8080

IOC Type: ipport

Threat Type: botnet_c2

Malware: C#-botnet

Confidence Level: Confidence level is High (100%)

Is compromised? Fato

ASN: AS21431 FENET

Country: BR

First seen: 2026-07-16 09:49:53 UTC

Last seen: never

UUID: 85c0d5a-763-191-976-4202a4000a

Reported by: 3 credits from ThreatFox

Revised by: 3 credits from ThreatFox

Tags: botnet, c2, malware, threatfox

Reference: https://github.com/0x00sec/0x00sec-research/blob/master/reports/0x00sec-report.md

5. Portas UDP mais recorrentes			
Porta	Assinantes	Regras	Observação
63	6	50	DNS – Investigar abuso
65535	5	58	QUIC/UDP-1400, comportamento incomum
1194	5	31	Porta padrão de OpenVPN, validar aplicação
1791	5	19	Porta associada a L2TP, revisar contexto
26568	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:

198.68.8.23

198.68.12.56

198.68.6.8

198.68.2.188

198.68.33.178

Eles compartilham várias ocorrências para:

UDP/65535, UDP/1194 e UDP/1701.

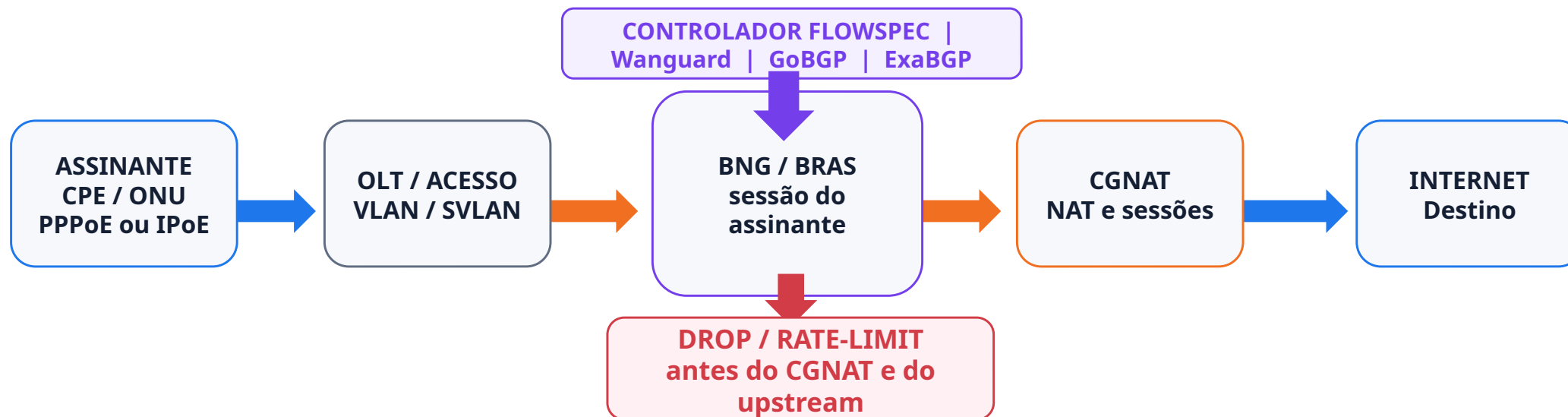
Entretanto, como alguns desses mesmos assinantes também apresentam tráfego para Roblox e outros serviços de jogos, esse grupo UDP deve ser tratado com menor confiança que o padrão TCP/23.

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

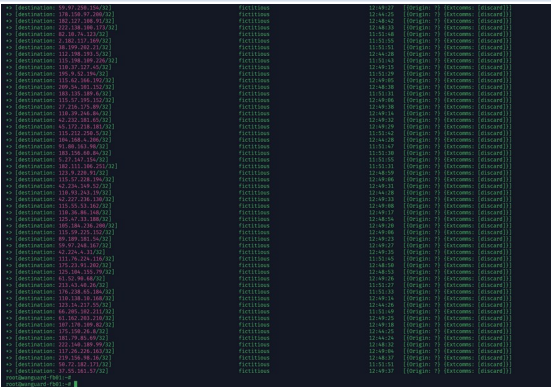
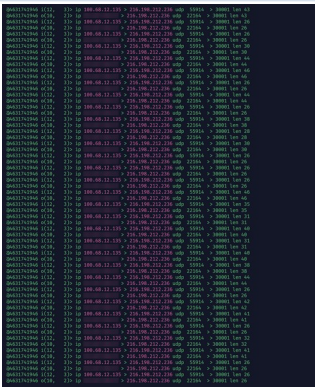
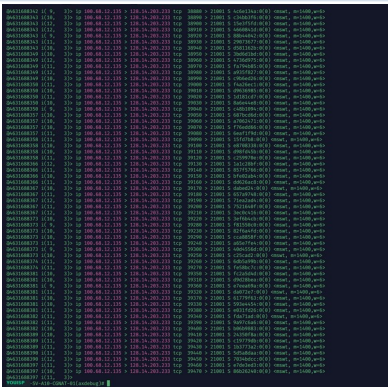
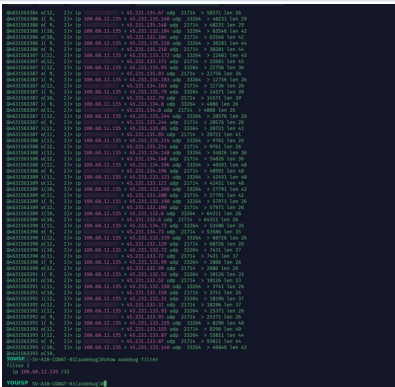
- Wanguard Filter, ACLs, NGFW ou scripts locais
- FlowSpec, listas e filtros por decoder
- rate-limit por sessão, CPS, portas e volume

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.



Profile	BGP Connection	Role	Status	Originator	From	Unit	FlowSpec	Comments	Action
100.68.2.128/32	FLOWSPEC-GORBP	Mitigation	✓	Anonymous #338712 (Filtering Rule #407625)	2025-08-01 10:37:00	=	source 100.68.2.128/32; destination 100.241.200.48/32; port 53; discard;	-	
100.68.11.130/32	FLOWSPEC-GORBP	Mitigation	✓	Anonymous #338711 (Filtering Rule #407625)	2025-08-01 10:37:05	=	source 100.68.11.130/32; destination 100.241.200.48/32; port 53; discard;	-	
			✓	Anonymous #338720 (Filtering Rule #407619)	2025-08-01 10:17:20	=	source 100.68.11.130/32; destination 100.48.88.116/32; port 53; discard;	-	
			✓	Anonymous #338724 (Filtering Rule #407625)	2025-08-01 10:17:31	=	source 100.68.11.130/32; destination 145.239.236.30/32; port 53; discard;	-	
			✓	Anonymous #338725 (Filtering Rule #407625)	2025-08-01 10:31:30	=	source 100.68.11.130/32; destination 37.225.90.116/32; port 53; discard;	-	
			✓	Anonymous #338726 (Filtering Rule #407625)	2025-08-01 10:32:19	=	source 100.68.11.130/32; destination 37.225.90.116/32; port 53; discard;	-	
			✓	Anonymous #338724 (Filtering Rule #407624)	2025-08-01 10:32:30	=	source 100.68.11.130/32; destination 37.225.90.116/32; port 53; discard;	-	
			✓	Anonymous #338725 (Filtering Rule #407624)	2025-08-01 10:37:59	=	source 100.68.11.130/32; destination 193.192.177.150/32; port 53; discard;	-	
			✓	Anonymous #338724 (Filtering Rule #407625)	2025-08-01 10:38:05	=	source 100.68.11.130/32; 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

