

SPEED FIBRA

PRODUTO COMERCIAL E OPERACIONAL

Proteção do Cliente Anti-Abuse & Filtro de Segurança

Documento mestre de projeto, implantação e operação
Versão com 2 VMs · Tráfego protegido · Sem limitar a velocidade do plano

Data: 13/08/2026

Versão do documento: 1.0

Público: Diretoria · NOC · Comercial · Suporte · Engenharia

Este PDF descreve **tudo o que precisa ser feito, como será feito**, quais **sistemas e softwares** entram no produto, e o que cada área precisa executar para a Speed Fibra oferecer proteção contra abuse, vírus, botnet, phishing e outros riscos — como **produto** para o cliente e para o provedor.

Nome comercial sugerido	Modelo técnico	Promessa ao cliente
Speed Protege · Speed Safe · Proteção Speed Fibra	2 VMs SafeDNS (HA) + Guardian + SpeedShield + Quarentena	Internet na velocidade do plano, com freio em ameaças

Sumário

1. Visão do produto (para qualquer pessoa entender)
2. Problema que resolvemos
3. O que o produto entrega (valor comercial)
4. Princípios e o que NÃO fazemos
5. Arquitetura completa (camadas de proteção)
6. Versão com 2 VMs — tráfego protegido
7. Sistemas e softwares necessários
8. Hardware e onde roda cada peça
9. Fluxos operacionais (dia a dia)
10. Integração com o que já existe na Speed Fibra
11. Plano de implantação por fases
12. Checklist detalhado de execução
13. Papéis e responsabilidades
14. Modelo comercial e comunicação com o cliente
15. Segurança, LGPD e boa prática de provedor
16. Monitoramento, métricas e sucesso
17. Riscos e mitigação
18. Glossário simples
19. Aprovação e próximos passos
20. Apêndice — ferramentas de proteção (mapa completo)

1. Visão do produto (para qualquer pessoa entender)

Imagine a internet do assinante como uma estrada. Hoje a Speed Fibra já tem **radares e barreiras na entrada da cidade** (proteção DDoS / SpeedShield) e um **centro de alertas** (Abuse Guardian + Telegram) quando alguém na rede está causando ou sofrendo abuso. O que ainda falta, como **produto**, é uma **guarda na porta da casa do cliente**: filtrar vírus, phishing e comunicação de botnet **sem reduzir a velocidade do plano e sem cortar a internet** na maioria dos casos.

Este produto une três frentes em uma oferta só:

- **Proteção do provedor** — menos IP em lista negra (RBL), menos ticket de abuse (EGP), menos vizinhos prejudicados no CGNAT.
- **Proteção do cliente** — menos vírus/phishing abrindo no navegador, menos IoT infectado “falando” com criminosos.
- **Oferta comercial** — plano ou add-on “Proteção Speed Fibra” (básico incluso / premium parental opcional).

A versão principal usa **duas máquinas virtuais (VMs)** em alta disponibilidade. Se uma cair, a outra mantém a proteção. O tráfego do cliente permanece na velocidade contratada; o que muda é que **domínios perigosos deixam de abrir**.

2. Problema que resolvemos

Problema	O que acontece hoje	Como o produto responde
PC/IoT infectado na casa do cliente	Gera spam, scan, botnet; pode listar o IP público do CGNAT e gerar ticket de abuse	Modo Filtro nas 2 VMs + alerta NOC; hard só se grave
Phishing / site de vírus	Cliente clica e infecta ou perde dados	Blocklist de malware/phishing no DNS seguro
DDoS de entrada no IP do cliente	Queda ou lentidão; ruído de alerta	SpeedShield mitiga; Guardian alerta só se ≥ 1000 Mbps e não mitigated
DDoS de saída (cliente ataca terceiros)	Risco ao AS e a outros clientes	Quarentena HARD no IP privado + derruba PPPoE
Alertas demais no Telegram	Equipe cansa e ignora	Filtros: mitigated skip, limiar 1000 Mbps, cooldown por IP
Cortar net de quem está infectado	Reclamação comercial; cliente fica sem serviço	Produto prefere filtrar e manter online na velocidade do plano

3. O que o produto entrega (valor comercial)

3.1 Para o cliente final

- Navegação com bloqueio de sites de malware e phishing (camada DNS).
- Internet continua na **velocidade do plano** — o filtro não é “freio de megas”.
- Em modo proteção reforçada (infectado suspeito): portal educativo em HTTP explicando o que fazer.
- Opcional premium: controle parental (adulto/ads) como upgrade comercial.

3.2 Para a Speed Fibra

- Menos IPs em RBL (CBL/Spamhaus) e menos tempo de resposta a abuse desks.
- Identificação correta do assinante atrás do CGNAT (100.64.x.x $\leftrightarrow$ 45.65.133.x).
- Ações graduais: avisar $\rightarrow$ filtrar $\rightarrow$ soft $\rightarrow$ hard.
- Produto vendável e diferenciador frente a concorrentes só “link puro”.
- Operação centralizada: painel /abuse, Telegram, Console NOC, Phoenix.

3.3 Nome e embalagem sugeridos

Camada	Nome sugerido	Incluso?
Base (todos ou opt-in)	Speed Protege Essencial	DNS seguro malware/phishing
Reforço automático (infectado)	Speed Protege Isolamento Inteligente	Listas agressivas + portal
Add-on comercial	Speed Protege Família	Parental / adulto / ads
Operação interna	NOC Abuse Desk	Guardian + hard/soft + RBL

4. Princípios e o que NÃO fazemos

4.1 Princípios

- **Proteger sem humilhar o cliente** — preferir filtro e educação a corte seco.
- **Nunca rate-limitar o plano como “antivírus”** — velocidade contratada permanece.
- **Nunca punir o CGNAT público inteiro** — sempre mirar o IP privado / login correto.
- **Alta disponibilidade** — 2 VMs para o filtro não sumir quando uma reinicia.
- **Humano no loop em ações graves** — hard automático só com política clara (hoje auto-hard desligado por padrão).
- **Transparência operacional** — tudo auditável (logs, painel, Telegram, notas na console).

4.2 Fora de escopo da v1 do produto

- Descriptografar HTTPS do cliente (MITM) — não faremos na v1.
- Substituir antivírus instalado no PC do cliente.
- Garantir bloqueio de malware que fala só com IP numérico (sem DNS) — fase 2 ou hard se abuso grave.
- Substituir o SpeedShield (DDoS de borda) — são complementares.

5. Arquitetura completa (camadas de proteção)

O produto não é um software único. É um **sistema em camadas**. Cada camada tem dono, ferramenta e modo de falha diferente. Juntas formam a proteção Speed Fibra.

Camada	Nome	Estado	Função em linguagem simples
A	SpeedShield	Já em produção	Escudo contra DDoS na borda da rede
B	Abuse Guardian	Já em produção	Detecta abuso e avisa no Telegram/NOC
C	Quarentena hard/soft	Já em produção	Corta ou limita HTTP de um IP privado no MikroTik
D	Scan RBL CGNAT	Já em produção	Verifica se IP público entrou em lista negra
E	Painel NOC /abuse	Já em produção	Tela para o técnico agir
F	SafeDNS 2 VMs	A construir (produto)	Filtra vírus/phishing sem cortar velocidade
G	Console + Notas + IA	Já em produção	Operação e documentação viva

Leitura rápida: **A–E e G já existem**. O salto de produto é a **camada F** (2 VMs) e a amarração comercial + política de quando usar filtro vs hard.

5.1 Diagrama lógico do fluxo

Casa do cliente → PPPoE (100.64.x.x) → **Rede Speed Fibra** → DNS forçado para **safedns-a / safedns-b** → se domínio bom, internet normal; se domínio mau, bloqueio/porta. Em paralelo: **SpeedShield** olha DDoS; **Guardian** olha abuso e pode pedir filtro, soft ou hard no **MikroTik**.

6. Versão com 2 VMs — tráfego protegido

Esta é a versão principal do produto de filtro. Duas VMs iguais formam o plano de DNS seguro. O cliente **não perde megas**; perde apenas o acesso a destinos classificados como ameaça (ou categorias parentais, se contratadas).

6.1 As duas máquinas

Item	VM 1 — safedns-a	VM 2 — safedns-b
Papel	Primária (ativa)	Secundária (HA / mesma função)
O que roda	Resolver DNS + RPZ/blocklist + portal + API	Cópia igual (sync de config/listas)
Se cair	Clientes usam a B (DNS2)	Clientes ficam na A
Onde	ESXi2 · datastore ssd03 (preferencial)	Mesmo host/cluster conforme capacidade
Tamanho sugerido	4 vCPU · 8 GB RAM · 40–60 GB	Igual à VM 1

6.2 Como o tráfego fica protegido (passo a passo)

1. O cliente autentica PPPoE e recebe IP privado CGNAT (100.64.x.x).
2. O concentrador/DHCP/PPPoE entrega DNS1=safedns-a e DNS2=safedns-b (ou VIP).
3. Reforço no MikroTik: redireciona ou restringe porta 53 (DNS) para as 2 VMs — evita furar com 8.8.8.8.
4. As VMs consultam listas de malware/phishing/C&C; (atualizadas automaticamente).
5. Domínio bom → resposta normal → site abre na velocidade do plano.
6. Domínio mau → NXDOMAIN ou IP do portal HTTP explicativo.
7. Se o caso for grave (DDoS de saída / EGP recorrente), o NOC aplica HARD no MikroTik (corta e derruba PPPoE).

6.3 Modos por cliente

Modo	O que o cliente sente	Quando usar
Normal / Essencial	Internet normal; bloqueio base de malware	Maioria dos assinantes (se política incluir base)
Filter (reforço)	Alguns sites ruins não abrem; portal se aplicável; velocidade cheia	Infectado, RBL, suspeita de botnet
Soft	HTTP limitado (já existe no MikroTik)	Observação leve sem filtro DNS ainda
Hard	Sem internet; PPPoE derrubado	Abuso grave de saída / reincidência EGP

7. Sistemas e softwares necessários

7.1 Já existentes (reutilizar)

Sistema	Onde	Software / peça	Uso no produto
SpeedShield	VM ~45.65.135.149	Plataforma DDoS + MikroTik	Mitigação DDoS entrada
Abuse Guardian	Hub 45.65.135.180	Python abuse_guardian.py	Deteção + Telegram
CGNAT Abuse	Mesmo monitor	abuse_cgnat.py	Mapear público↔privado, quarentena
MikroTik BGP/CCR	45.65.132.1 e PPPoE	RouterOS address-list + filter	hard/soft + redirect DNS
Painel Abuse	noc.aspeednet.com.br/abuse	NOC web	Operação humana
Phoenix	NOC	Monitoramento	Health das VMs e serviços
Console Speed Fibra	/console/	app Python + Notas	Operação e documentação
Telegram	Bot alertas	Bot API	Aviso multi-usuário/grupo
IXC / PPPoE	SGP/IXC + concentrador	Sessões, login	Identificar assinante e provisionar DNS

7.2 Novos (a instalar nas 2 VMs)

Componente	Opções de software (recomendado em destaque)	Para que serve
Sistema operacional	Debian 12/13 ou Ubuntu LTS (recomendado: Debian)	Base estável das VMs
Resolver DNS com RPZ	Unbound ou BIND 9 com RPZ; alt.: AdGuard Home / Technitium	Aplicar blocklists e responder aos clientes
Atualizador de listas	Scripts cron + fontes públicas (URLhaus, ThreatFox, DBL, OISD etc.)	Manter bloqueios atualizados
Portal HTTP	Nginx + página estática/simples	Avisar cliente quando bloquear
API de política	Python (FastAPI/Flask) ou integração no monitor	Marcar login/IP em modo filter
Sync A↔B	rsync/git/ansible + healthcheck	As 2 VMs iguais
Observabilidade	node-exporter + logs + checagem DNS	Phoenix/alerta se filtro cair
Certificados	Let's Encrypt (portal/API se HTTPS)	Portal seguro para gestão

7.3 Fontes de inteligência (listas)

- Malware e phishing: URLhaus, ThreatFox, Spamhaus DBL e feeds confiáveis equivalentes.
- Conteúdo opcional parental: categorias (adulto, ads) — somente no add-on comercial.
- Processo: baixar → validar → publicar nas 2 VMs → métrica de quantos domínios ativos.
- Regra: lista com falso positivo alto deve ter exclusão rápida (allowlist NOC).

7.4 Softwares que o cliente NÃO precisa instalar

O produto é **na rede do provedor**. O cliente não precisa instalar agent. Isso é vantagem comercial: funciona em TV, celular, IoT e PC sem app.

8. Hardware e onde roda cada peça

Peça	Host / local	Recursos	Observação
safedns-a e safedns-b	ESXi2 (10.100.99.3), disco ssd03	4 vCPU / 8 GB / 40–60 GB cada	Par HA do produto

Peça	Host / local	Recursos	Observação
Abuse Guardian + APIs	Hub nextcloud 45.65.135.180	Já existente	Timers systemd 10 min / RBL horário
Ollama / Chat IA NOC	Hub :11434	Já existente	Apoio operacional, não é o filtro
Grok / engenharia	VM 45.65.135.187	Já existente	Implementação e shell da console
SpeedShield	VM 149 (ESXi2)	Já existente	DDoS
MikroTik BGP + PPPoE	45.65.132.1 / .118	Hardware de rede	Listas e enforce DNS

9. Fluxos operacionais (dia a dia)

9.1 Fluxo A — Cliente limpo com proteção essencial

- DNS do cliente aponta para as 2 VMs (ou VIP).
- Listas base bloqueiam malware/phishing conhecidos.
- Sem ticket, sem Telegram de abuso.

9.2 Fluxo B — Suspeita de infecção / RBL

- Guardian detecta (RBL infecção real, não PBL; ou comportamento de saída anômalo).
- Identifica candidatos CGNAT e ranqueia o login mais suspeito.
- Telegram para NOC com tipo, IP público, privado, login e passo a passo.
- Ação preferencial do produto: **mode=filter** nas 2 VMs (listas agressivas + portal).
- Suporte orienta reinício de roteador, desligar IoT suspeito, antivírus no PC.
- Após limpeza RBL + período sem reincidência → volta ao modo normal.

9.3 Fluxo C — DDoS de saída / abuso grave

- Identificar IP privado e login (nunca bloquear só o público CGNAT “no escuro”).
- Quarentena HARD: address-list abuse-quarantine + drop + remove PPPoE.
- Contato comercial/suporte; só liberar após mitigação na casa do cliente.

9.4 Fluxo D — DDoS de entrada

- SpeedShield mitiga na borda.
- Guardian só alerta se volume relevante (≥ 1000 Mbps) e não mitigated (anti-spam).
- Não é função do SafeDNS “parar DDoS” — são sistemas diferentes.

10. Integração com o que já existe na Speed Fibra

Sistema atual	Como integra no produto
abuse_guardian.py	Novo resultado de ação: filter (além de soft/hard); mensagens Telegram atualizadas
abuse_cgnat.py	API/listas: colocar privado em grupo DNS filter; manter hard/soft MikroTik
Telegram multi-chat	Mesmos destinos (grupo + operadores); textos com link do portal e /abuse
noc.aspeednet.com.br/abuse	Botões: Filtrar · Soft · Hard · Liberar
Console /console/	Notas e shell na VM Grok; monitor de health das safedns
Phoenix	Registrar as 2 VMs + checagens DNS/HTTP
IXC	Flag de produto no contrato; DNS option no provisionamento PPPoE
SpeedShield	Continua dono de DDoS; Guardian só consome eventos com filtro de spam

11. Plano de implantação por fases (o que fazer, na ordem)

Nada deve ser ligado em massa no primeiro dia. A ordem abaixo reduz risco e permite aprender com poucos clientes antes de virar produto geral.

Fase 0 — Decisão e preparação (1–3 dias)

- Aprovar nome comercial e se a proteção essencial será default ou opt-in.
- Aprovar política: infectado vai primeiro para FILTER (recomendado) ou HARD.
- Reservar IPs/VLAN e recursos no ESXi2 (ssd03).

- Definir donos: Engenharia, NOC, Comercial, Suporte.

Fase 1 — MVP SafeDNS com 2 VMs (3–7 dias)

- Criar safedns-a e safedns-b no ESXi2.
- Instalar SO + Unbound/BIND RPZ (ou AdGuard) + Nginx portal.
- Publicar 1–2 listas malware confiáveis + cron de atualização.
- API mínima: adicionar/remover IP ou login no modo filter.
- Teste de bancada com 1 login laboratório (não produção massiva).
- Healthcheck + registro no Phoenix.

Fase 2 — Enforce DNS controlado (2–5 dias)

- PPPoE de lab entrega DNS das 2 VMs.
- No MikroTik lab: redirect 53 dos IPs de teste.
- Validar que 8.8.8.8 não fura o filtro nos clientes de teste.
- Medir latência DNS e falsos positivos.

Fase 3 — Integração Guardian + painel (3–7 dias)

- Implementar mode=filter no fluxo de quarentena/ações.
- Botão no /abuse e textos no Telegram.
- Runbook de suporte (script de atendimento).
- Piloto com N clientes reais (ex.: 20–50) ou só sob incidente.

Fase 4 — Produto comercial (1–2 semanas)

- Cadastro no IXC (plano/add-on).
- Material de venda e FAQ do cliente.
- Opcional parental (Família).
- Default de rede (se aprovado) para base Essencial.
- Treinamento suporte N1/N2.

Fase 5 — Endurecimento contínuo

- Métricas semanais: bloqueios, falsos positivos, tickets EGP, tempo em hard.
- Melhoria de listas e allowlist.
- Avaliar fase 2 técnica: SNI/firewall seletivo (sem MITM completo).
- Revisão de capacidade das VMs (CPU/RAM/qps DNS).

12. Checklist detalhado de execução

12.1 Checklist de infraestrutura

- ☐ ESXi2 com espaço em ssd03 para 2 VMs
- ☐ IPs de gestão e DNS definidos (documentar em INVENTORY)
- ☐ Backup/snapshot antes de mudanças MikroTik
- ☐ Acesso SSH chave entre hub, grok e VMs novas
- ☐ NTP, logs e atualizações de segurança do SO

12.2 Checklist de software das VMs

- ☐ SO instalado e hardened (ssh chave, firewall local)
- ☐ Resolver DNS com RPZ/blocklist funcionando
- ☐ Teste: dig @safedns dominio-seguro → OK; dominio-malware-de-teste → bloqueado
- ☐ Portal HTTP responde
- ☐ Cron de listas OK nas duas VMs
- ☐ Sync A↔B verificado
- ☐ node-exporter / health no Phoenix

12.3 Checklist de rede

- ☐ Clientes lab com DNS A/B
- ☐ Redirect/restrição porta 53 testada só no lab
- ☐ Medição de latência DNS antes/depois
- ☐ Plano de rollback (voltar DNS e tirar redirect) documentado e testado

12.4 Checklist de operação

- ☐ Runbook N1: o que dizer ao cliente em modo filter
- ☐ Runbook N2: quando escalar para hard
- ☐ Telegram com textos novos validados
- ☐ Painel /abuse com ações filter/soft/hard/liberar
- ☐ Treinamento de 1 hora com suporte e NOC

12.5 Checklist comercial

- ☐ Nome e preço do add-on (se houver)
- ☐ Texto de contrato / regulamento (o que é bloqueado)
- ☐ FAQ site e script de vendas
- ☐ Política de desativação a pedido do cliente (opt-out) se a base for default

13. Papéis e responsabilidades (quem faz o quê)

Papel	Responsabilidades
Engenharia / Grok / Rede	Criar VMs, software DNS, APIs, integração Guardian, MikroTik lab→prod, documentação técnica
NOC	Operar alertas, aplicar filter/soft/hard, liberar, acompanhar RBL, health das VMs
Suporte N1	Orientar cliente em modo filter; checklist de limpeza de PC/IoT; abrir N2 se reincidir
Suporte N2 / Abuse desk	Casos EGP, hard, evidências, liberação condicionada
Comercial	Empacotar produto, preço, argumentário, evitar promessa de "antivírus total"
Diretoria	Aprovar política (default filter vs hard), investimento de VMs, go-live

14. Modelo comercial e comunicação com o cliente

14.1 Como falar sem jargão

“A Speed Fibra oferece uma camada extra de proteção na rede: sites conhecidos por vírus e golpes deixam de abrir. Sua velocidade de plano continua a mesma. Se detectarmos atividade perigosa vinda da sua conexão, podemos reforçar o filtro e te avisar para verificar computadores e dispositivos da casa.”

14.2 O que NÃO prometer

- “Nunca vai ter vírus” — impossível e gera processo.
- “Bloqueamos todo conteúdo ruim na internet” — listas erram; existe allowlist e evolução.
- “É um antivírus instalado” — é proteção de rede/DNS.

14.3 Quando o cliente reclamar que “não abre um site”

- NOC verifica se o domínio está na blocklist (falso positivo).
- Se legítimo: allowlist em minutos e registro do caso.
- Se realmente malware: explicar e manter bloqueio.

15. Segurança, LGPD e boa prática de provedor

- Tratar logs de DNS/abuse com acesso restrito (só NOC/engenharia).
- Não expor dados de um cliente em Telegram de forma desnecessária (login/IP sob política interna).
- Informar no contrato/regulamento a existência de filtragem de segurança e parental opcional.
- Manter opt-out quando a legislação/contrato exigirem para categorias não relacionadas a segurança.
- Bloqueios de segurança (malware/C&C;) são legítimos para proteção da rede e do próprio assinante.
- Retenção de logs com prazo definido (ex.: 30–90 dias) e backup controlado.

16. Monitoramento, métricas e sucesso

Métrica	Meta / leitura
Disponibilidade safedns-a e b	≥ 99,9% mensal; nunca as duas down juntas
Latência DNS p95	Não degradar sensivelmente vs baseline (definir número no lab)
Tickets EGP / IPs em RBL infecção	Tendência de queda após go-live
Falsos positivos/semana	Baixos e com tempo médio de correção < 1h útil
Tempo médio em HARD	O menor possível; preferir FILTER
Alertas Telegram úteis	Menos spam (já com 1000 Mbps + skip mitigated)
Clientes no add-on Família	Métrica comercial (se lançar)

17. Riscos e mitigação

Risco	Mitigação
As 2 VMs caírem	Phoenix crítico; rollback DNS; capacidade ESXi monitorada
Falso positivo em site bancário/gov	Allowlist prioritária; listas maduras; processo N2
Cliente fura com DNS público	Redirect/restrição 53 no MikroTik (fase de rede)
Malware só por IP (sem DNS)	Hard se abuso ativo; fase 2 de firewall seletivo
Sobrecarga de QPS DNS	Cache, dimensionar vCPU, anycast futuro se crescer
Equipe aplicar hard em massa	Política escrita; auto-hard off; auditoria
Cliente achar que “a Speed espia HTTPS”	Comunicação clara: sem MITM; só DNS/categorias

18. Glossário simples

Termo	Significado simples
Abuse	Uso abusivo da rede (spam, ataque, botnet, scan)
RBL	Lista negra pública de IPs que mandam spam/malware
CGNAT	Vários clientes compartilham um IP público; dentro usam 100.64.x.x
PPPoE	Login da conexão do assinante na fibra
DNS	Serviço que transforma nome do site em caminho na internet
RPZ / blocklist	Lista de nomes que o DNS se recusa a abrir
Hard	Corta a internet daquele IP/login

Termo	Significado simples
Soft	Ainda tem net, mas HTTP fica limitado
Filter	Net na velocidade do plano; bloqueia ameaças no DNS
SpeedShield	Proteção DDoS da borda Speed Fibra
Guardian	Robô que detecta abuso e avisa o time
HA	Alta disponibilidade (uma VM cobre a outra)
EGP	Organismo/processo de denúncia de abuse na internet

19. Aprovação e próximos passos

Este documento serve como **especificação de produto e plano de obra**. Para sair do papel, a Speed Fibra precisa de três decisões e uma execução.

19.1 Decisões necessárias

- **Política:** infectado vai para FILTER por padrão? (recomendado: sim)
- **Comercial:** Essencial default para todos ou só add-on?
- **Go-live:** data alvo da Fase 1 (2 VMs lab) e do piloto.

19.2 Primeira execução técnica (quando aprovado)

- Criar safedns-a e safedns-b no ESXi2 (ssd03).
- Instalar resolver + listas + portal + API.
- Testar 1 login lab de ponta a ponta.
- Só então integrar Guardian mode=filter e Telegram.

19.3 Contatos e artefatos vivos

Artefato	Onde
Este PDF	exports/ + downloads NOC (ver abaixo)
Console Notas Grok	https://noc.aspeednet.com.br/console/ (aba Notas Grok)
Painel Abuse	https://noc.aspeednet.com.br/abuse
SpeedShield	https://noc.aspeednet.com.br/speedshield/
Código Guardian	/opt/speedfibra-monitor/abuse_guardian.py (hub)
Código CGNAT	/opt/speedfibra-monitor/abuse_cgnat.py (hub)
Export histórico Grok	https://noc.aspeednet.com.br/downloads/grok-export/

20. Apêndice — ferramentas de proteção (mapa completo do produto)

Lista única para quem for montar o “kit de proteção Speed Fibra” — do que já roda ao que será comprado/criado em software livre ou interno.

Ferramenta	Tipo de proteção	Status
SpeedShield	DDoS de borda / mitigação	Produção
MikroTik address-list hard/soft	Isolamento e limite HTTP seletivo	Produção
Abuse Guardian + RBL	Deteção, alerta, investigação CGNAT	Produção
Telegram multi-destino	Operação em tempo real	Produção

Ferramenta	Tipo de proteção	Status
Painel /abuse	Ação humana	Produção
Console + Notas + Shell Grok	Operação e documentação	Produção
Phoenix	Monitoramento de saúde	Produção
SafeDNS VM A + VM B	Filtro malware/phishing/C&C; (e parental opcional)	A construir
Listas de inteligência	Atualização de ameaças	A conectar no SafeDNS
Portal do cliente (HTTP)	Educação / aviso de bloqueio	A construir
API policy filter	Automação mode=filter	A construir
IXC produto/add-on	Comercialização	A configurar
Redirect DNS 53	Impedir bypass do filtro	A implantar (lab→prod)
Allowlist NOC	Corrigir falso positivo rápido	A formalizar processo

Speed Fibra — Produto Proteção do Cliente / Anti-Abuse · Documento v1.0 · Gerado em 13/08/2026 10:55 · Elaborado para compreensão multipúblico (diretoria, comercial, suporte e engenharia).