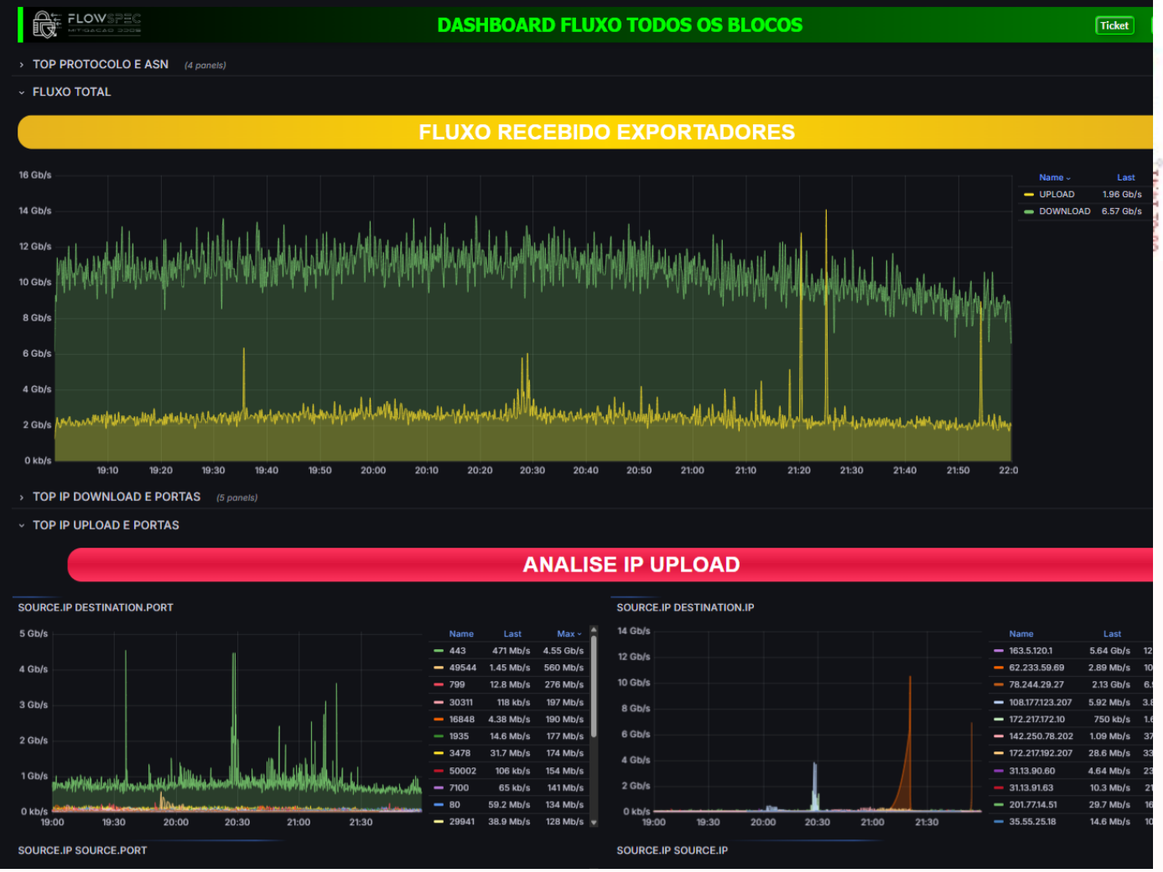
```
root@wanfilter:~# ethtool --show-ntuple enp33s0f0np0
63 RX rings available
Total 7 rules

Filter: 16
        Rule Type: Raw IPv4
        Src IP addr: 92.223.84.33 mask: 0.0.0.0
        Dest IP addr: [redacted] mask: 0.0.0.254
        TOS: 0x0 mask: 0xff
        Protocol: 6 mask: 0x0
        L4 bytes: 0x0 mask: 0xffffffff
        Action: Drop
```



FLOWSPEC
MITIGAÇÃO DDOS

AS61620

Wanguard Anti-DDoS

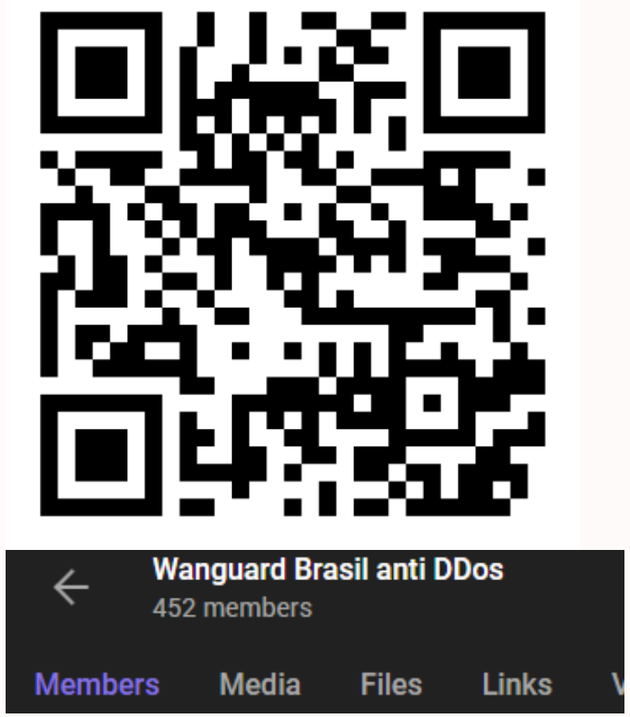
Monitoramento Inteligente, Mitigação Automática e Integração Completa para ISPs

Palestrante: Raphael Rodrigues

COMUNIDADE WHATSAPP E TELEGRAM WANGUARD BRASIL

GRUPO WHATSAPP

GRUPO TELEGRAM



STREAM PODCAST

O QUE NOS ESPERA!

O cenário crítico dos ataques DDoS

Wanguard: Arquitetura de Defesa

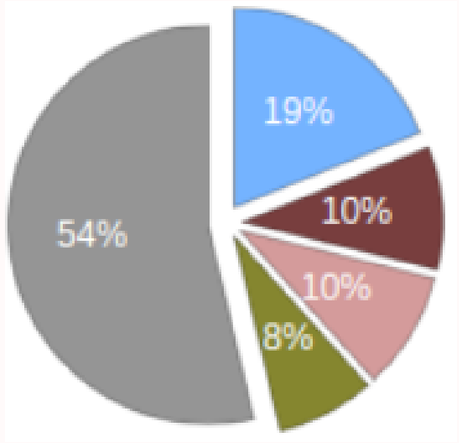
Detecção Inteligente de Anomalias

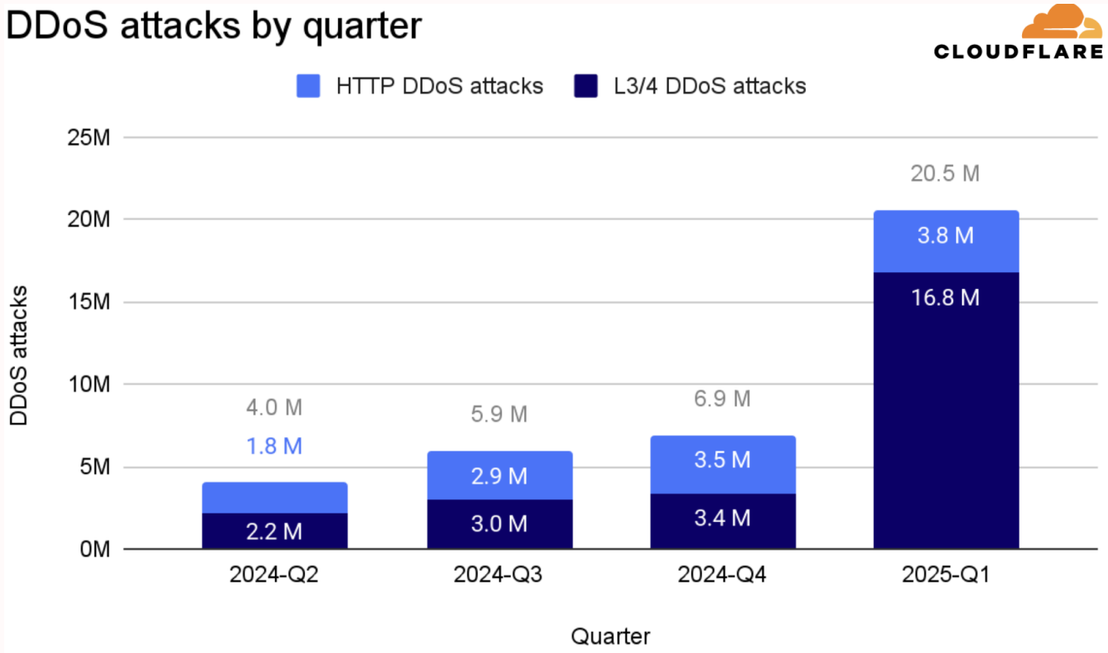
Métodos de mitigação local

Integração com sua Infraestrutura

Recomendação e próximos passos

O Cenário Crítico dos Ataques DDoS





Provedores de internet e empresas enfrentam uma escalada sem precedentes de ataques distribuídos que ameaçam a continuidade dos negócios.

Crescimento Exponencial

Ataques DDoS aumentaram 300% nos últimos anos:
54% ATAQUES VIA IXBR
19% ATAQUES VIA PNI
18% ATAQUES VIA TRANSITO IP

Impacto Financeiro

Indisponibilidade causa perda média de R$ 50 mil por hora, além de danos irreparáveis à reputação e êxodo de clientes

Defesa Inteligente

Soluções manuais são insuficientes

— a mitigação moderna exige análise comportamental automatizada e resposta em tempo real

Wanguard: Arquitetura de Defesa

Uma solução modular completa que combina monitoramento avançado, análise inteligente e mitigação automática através de componentes integrados.

WANsensor

Captura e análise de NetFlow/sFlow/SPAN em tempo real com perfis comportamentais dinâmicos

WANfilter

Mitigação automatizada via BGP Flowspec, Hardware Offload, Netfilter, DPDK Filter

WANsupervisor

Interface centralizada para gerenciamento, relatórios e visualização de ameaças

WANbgp

Integração nativa com roteadores de borda para anúncios BGP automatizados

Compatibilidade Universal: Huawei, Juniper, Mikrotik, Cisco e demais fabricantes de roteadores enterprise

Detecção Inteligente de Anomalias

O Wanguard vai além de thresholds estáticos, utilizando análise comportamental avançada..

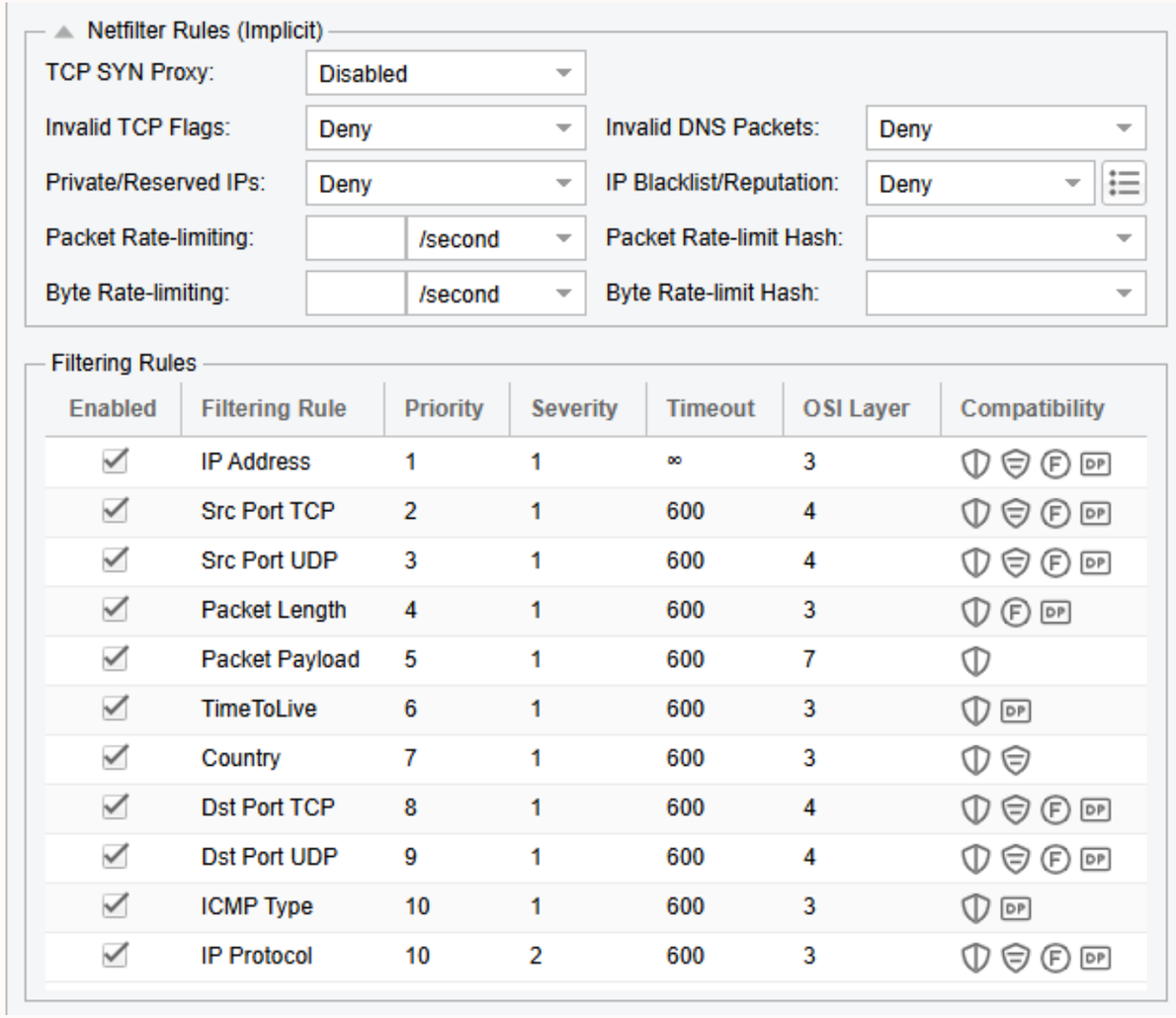
Análise Multidimensional

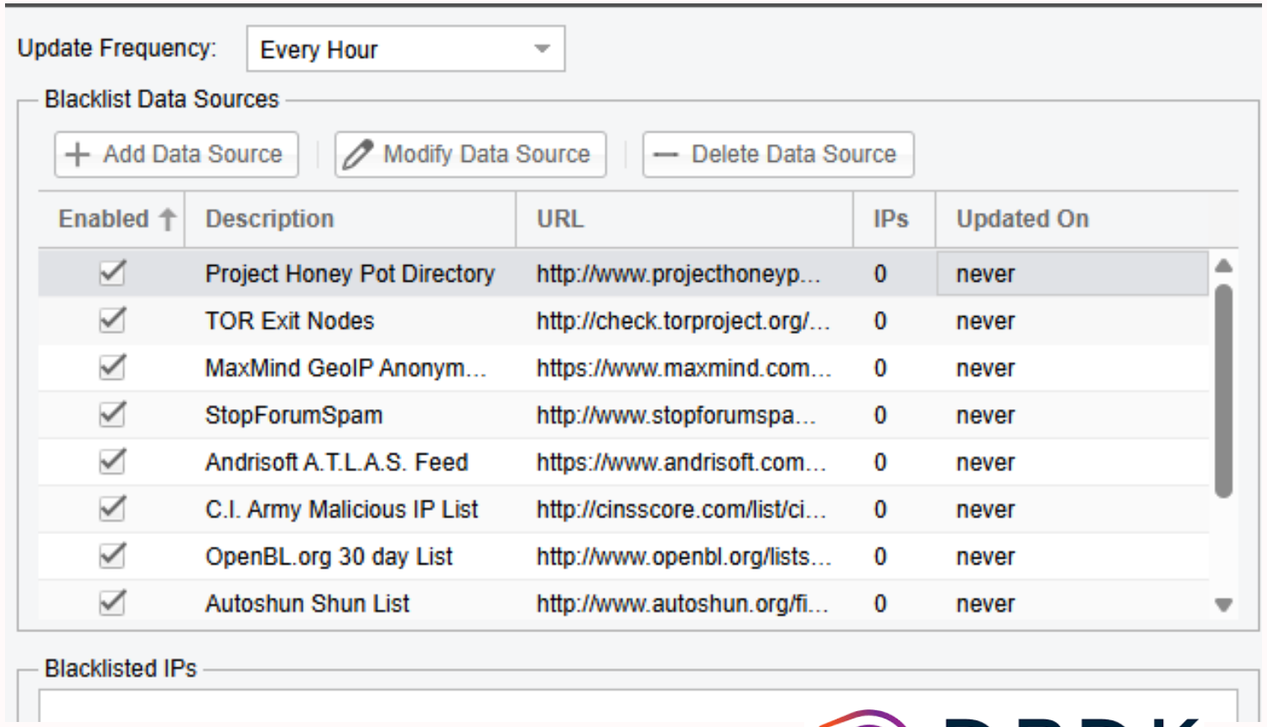
- Thresholds dinâmicos baseados em perfis históricos e padrões de tráfego legítimo
- Correlação de dados NetFlow/SPAN PORT com feeds externos de reputação

Possível Integração

- MISP: Indicadores de comprometimento compartilhados globalmente
- AbuseIPDB: Reputação de IPs maliciosos em tempo real
- Spamhaus: Listas de bloqueio de botnet e spam

Métodos de mitigação local





FLOWSPEC

DPDK
LANE DEVELOPMENT KIT

OFFLOAD

netfilter
firewalling, NAT, and packet mangling for linux

intel

Mellanox
TECHNOLOGIES

Mitigação Automática em Tempo Real

Do momento da detecção até a neutralização da ameaça em segundos.

Detecção

Anomalia identificada através de análise Comportamental e thresholds

Classificação

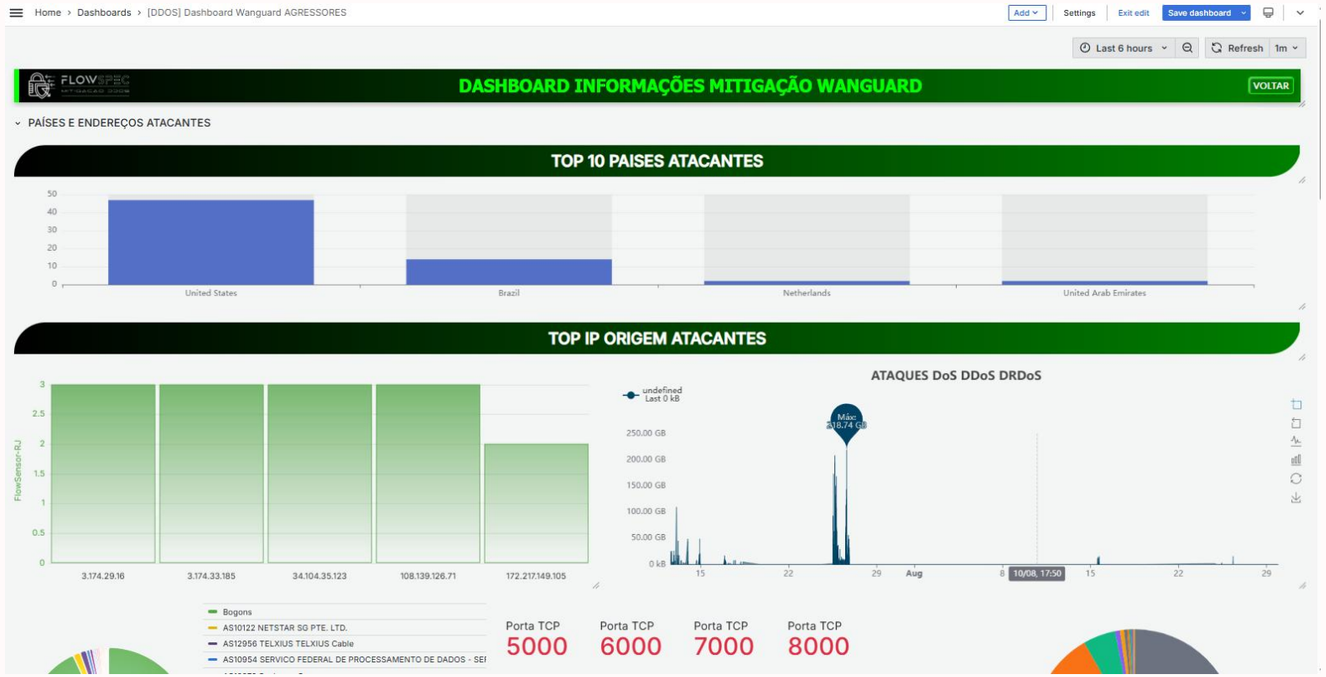
Tipo de ataque, origem e alvo determinados automaticamente

Anúncio BGP

Anúncios BGP via GoBGP/ExaBGP para roteadores

Limpeza

Tráfego malicioso descartado , tráfego legítimo flui. DPDK, OFFLOAD, NETFILTER, FLOWSPEC



Estratégias Híbridas

Combine mitigação local para ataques menores com scrubbing centers em nuvem para ataques volumétricos superiores a 100 Gbps, otimizando custos e eficiência.

Resposta em Segundos

Tempo médio de mitigação de 5-25 segundos desde a detecção inicial até o bloqueio efetivo, minimizando janela de impacto.

Visualização com Grafana

Dashboards personalizados que transformam dados brutos em inteligência acionável para equipes de segurança e operações SOC/NOC.

Tráfego em Tempo Real

Visualização de bits/pps por sensor com alertas configuráveis e histórico de tendências

Origem dos Ataques

Top ASN atacantes, distribuição geográfica e correlação com indicadores de ameaças

Análise de Vetores

Classificação por tipo de ataque: SYN flood, UDP amplification, HTTP flood e volumétricos

Integração Total com sua Infraestrutura

APIs abertas e protocolos padrão garantem que o Wanguard se encaixe perfeitamente no ambiente tecnológico do seu ISP.

Visualização Avançada

Grafana: Dashboards customizados com métricas de tráfego, alertas em tempo real e relatórios históricos para análise forense

Anúncios BGP Dinâmicos

Flowspec / Desvio: Propagação automática de anúncios BGP para roteadores de borda sem intervenção manual

Automação via API REST

Integração com sistemas de ticket (SOC/NOC), SIEM, e ferramentas de orquestração para workflows automatizados

Pipeline de Automação Completo

Logs coletados → Alerta gerado → Mitigação executada → Ticket criado → Relatório enviado — tudo sem intervenção humana


```
{
 "alert": {
 "sensor_id": "SP-CORE-01",
 "attack_type": "SYN_FLOOD",
 "target_ip": "200.x.x.x",
 "volume_gbps": 45.2,
 "mitigation_status": "active",
 "flowspec_rules": ["block tcp syn 200.x.x.x/32"]
 }
}
```

Andrisoft
Network Security

Log in

Home | Software | Hardware | Download | Store | Support | Partners | Company

Home ▸ Store ▸ Software Licenses

SOFTWARE LICENSES

$595.00 each
Wanguard Sensor license

$995.00 each
Wanguard Filter license

$345.00 each
Wansight Sensor license

$1,410.00 each
DPDK Engine license

CURRENCY SWITCHER

$ USD

YOUR CART

The cart is empty

Casos Reais de Sucesso

Provedores brasileiros já protegem suas redes e clientes com eficiência comprovada.

AUMENTO

Tempo de Disponibilidade

Após implementação em ISPs de médio porte

15seg~

Tempo Médio de Resposta

Da detecção até mitigação completa

120Gb

Maior Ataque Mitigado

Ataque volumétrico neutralizado com sucesso

85%

Redução de Custos

Em downtime e perda de receita operacional

Proteção Contra Botnets

Detecção e bloqueio efetivo de famílias conhecidas:

- Mirai: Ataques volumétricos de dispositivos IoT comprometidos
- Mozi: Botnet P2P com milhões de dispositivos infectados
- Gafgyt: Ataques direcionados a infraestrutura de ISPs

Search Botnets

Integração exclusiva com ferramenta da Flowspec Solutions para identificação proativa de dispositivos comprometidos na sua rede antes que sejam utilizados em ataques.

Da Visibilidade à Ação Proativa Recomendação

Monitoramento 24/7

Visibilidade total do tráfego com análise comportamental contínua e perfis dinâmicos de cada segmento da rede

Mitigação Inteligente

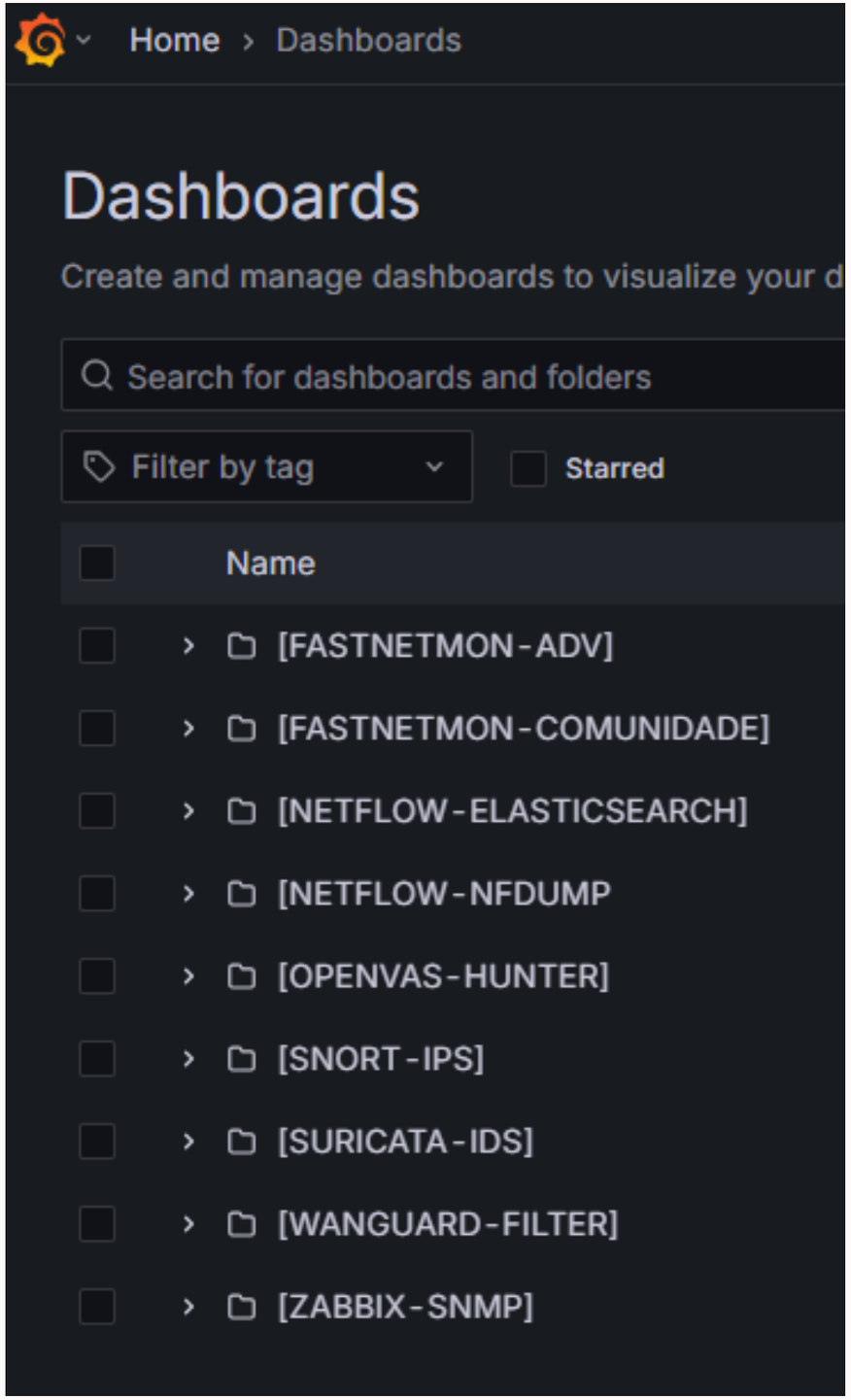
Resposta automática baseada em regras personalizáveis, machine learning e inteligência de ameaças global

Inteligência de Ameaças

Correlação com feeds externos, detecção de botnets e antecipação de novos vetores de ataque emergentes

---

ISPs que investem em defesa proativa conquistam vantagem competitiva significativa: maior confiabilidade do serviço, redução de custos operacionais, proteção da reputação e satisfação superior dos clientes.



Próximos Passos

Experimente o Wanguard na sua Rede

A Flowspec Solutions oferece POC gratuita e treinamento técnico avançado para sua equipe de operações e segurança.

01

Análise de Ambiente

Avaliação da infraestrutura atual e definição de objetivos

02

POC Gratuita

Implementação piloto de 30 dias com suporte técnico completo

03

Treinamento Técnico

Capacitação da equipe em operação e otimização avançada

04

Implementação Completa

Deploy em produção com monitoramento e suporte contínuo

- Entre em contato: Nossa equipe de especialistas está pronta para demonstrar como o Wanguard pode proteger sua infraestrutura

YouTube @raphaelisp

FLOWSPEC
MITIGAÇÃO DDOS

https://flowspec.net.br/

FONTES & IMG:

https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/
https://stormwall.network/resources/blog/ddos-report-q1-2025
https://www.netscout.com/threatreport/global-highlights/
https://www.fastly.com/blog/ddos-in-april
https://www.akamai.com/blog/security/ddos-attack-trends-2024-signify-sophistication-overshadows-size
https://www.arelion.com/knowledge-hub/white-papers/ddos-threat-landscape-report-2025
https://thehackernews.com/2025/07/hyper-volumetric-ddos-attacks-reach.html
https://www.intel.com.br/content/www/br/pt/homepage.html
https://www.nvidia.com/en-us/networking/
https://www.dpdk.org/
https://grafana.com/
https://chatgpt.com/
https://claude.ai/
https://gemini.google.com/
https://www.akamai.com/blog/security/ddos-attack-trends-2024-signify-sophistication-overshadows-size
https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/
https://www.netscout.com/threatreport/global-highlights/

OBRIGADO!