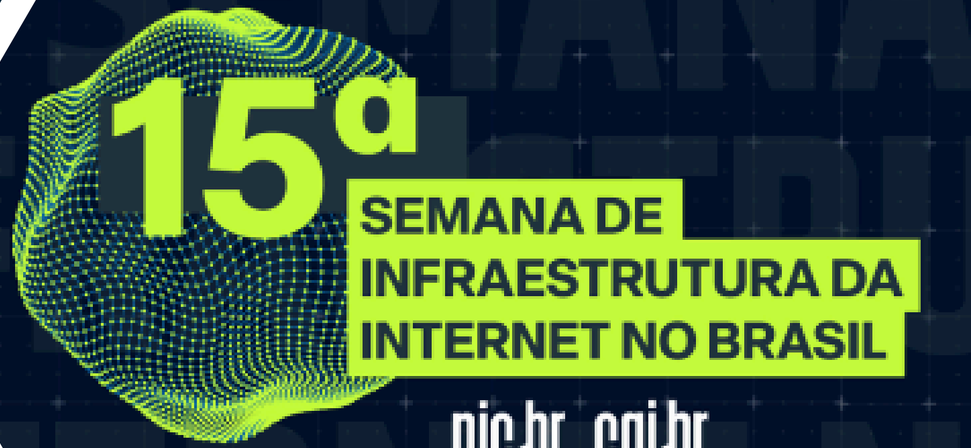
NEXTHOP SOLUTIONS

GTER 54

DDOS EM 2025

Obrigações das Redes, Observabilidade e Ações Indispensáveis aos ASNs



nic.br cgi.br

HTTPS://NEXTHOP.SOLUTIONS

NETWORK EDUCATION

ELIZANDRO PACHECO

Instrutor

Tecnologia, inovação e comunidade sempre foram minha paixão.

Sou graduado em Tecnologia de Marketing Digital pela Estácio, pós-graduando em Inteligência Artificial pela UniRitter e CEO da NextHop Solutions®, empresa Gaúcha que desde 2004 vem ajudando provedores de acesso a evoluírem no Brasil e no exterior.

Fundador e instrutor da Network Education®, autor do livro Docker para Provedores e palestrante nos maiores eventos do setor. Como desenvolvedor PHP e Python, especialista em sistemas Linux, minha missão é transformar conhecimento técnico em soluções práticas, confiáveis e rentáveis.

Fora do mundo da tecnologia, sou casado, pai de dois filhos e apaixonado por carros turbo e viagens de moto – porque nem só de ping vive um homem! 😂

elizandropacheco

+55 51 99871-8111

elizandropacheco

elizandropacheco

ERA UMA VEZ...

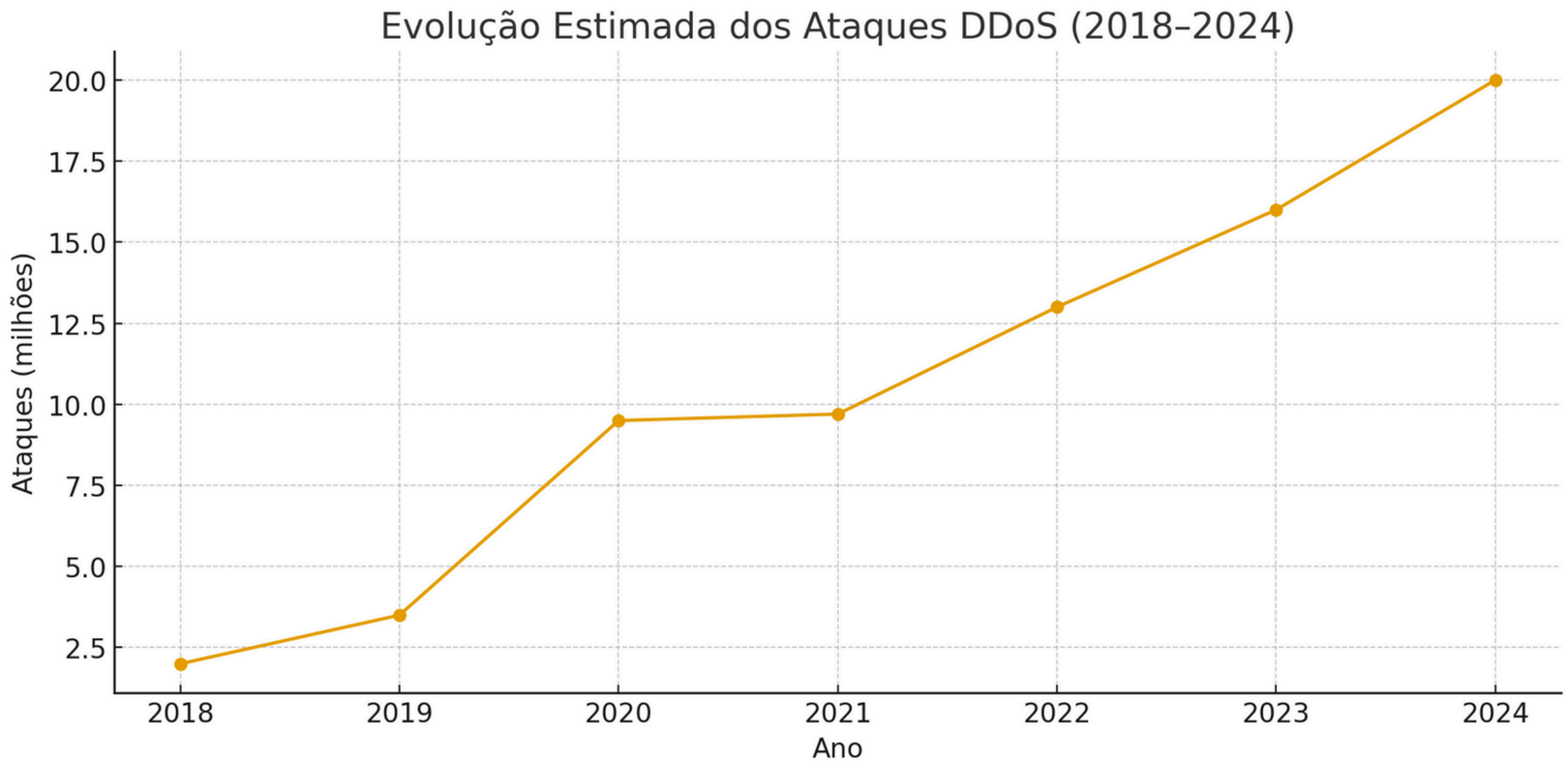
Em um mundo não tão distante

Ataques não são novidade!

O primeiro ataque distribuído de negação de serviço (DDoS) conhecido aconteceu em **1996**, quando o provedor de internet Panix em Nova York foi atacado por uma **inundação SYN**, ficando offline por vários dias. Antes disso, em 1999, houve um ataque de destaque usando a ferramenta "Trinoo" contra a Universidade de Minnesota, sendo considerado um dos primeiros grandes ataques DDoS significativos. Em 2000, um jovem conhecido como Mafiaboy realizou ataques DDoS que derrubaram sites importantes como Yahoo! e eBay, causando prejuízos financeiros expressivos. O primeiro ataque DDoS registrado como tal data de 1996, enquanto ataques DoS anteriores vieram desde a década de 1970 (com DoS, não distribuídos).

ERA UMA VEZ...

Em um mundo não tão distante



HTTPS://NEXTHOP.SOLUTIONS

ERA UMA VEZ...

Em um mundo não tão distante

E nos ISPs?

Nos ISPs, **ataques não são novidade**. E durante os últimos anos também sofreram as consequências dessa evolução.

Acompanhamos inúmeros casos durante esses 25 anos que atuamos exclusivamente com ISPs, e já passamos por situações das mais diversas...

Vimos desde extorções e cenários milhares de Reais gastos em soluções de mitigação, o nascimento e morte de soluções e empresas que trazem promessas milagrosas, até situações onde os custos de mitigação inviabilizavam o negócio.

A REALIDADE MUDOU

Não dá pra esperar o ataque chegar, pois ele vai chegar.

A realidade mudou.

E não há mais tempo pra **esperar acontecer** pra tomar uma ação.

Implementar **políticas de segurança**, seguir as boas práticas, ter um bom **sistema de detecção** e uma boa **nuvem de mitigação** é **primordial** nos dias atuais.

É uma jornada longa, em um mercado com muitas ofertas de soluções milagrosas criadas por aventureiros que podem transformar seu dia a dia em um verdadeiro inferno e acabar com seu negócio.

Mitigação e Prevenção carecem de boas orientações e de muita experiência.

HTTPS://NEXTHOP.SOLUTIONS

POR ONDE COMECAR?

Nem tudo depende de terceiros...

Antes de pensar em qual solução contratar para seu ISP, **arrume a casa**!

Nenhuma solução de mitigação será eficiente se sua rede for uma bagunça.

Há 10 anos, neste mesmo evento, mais especificamente na **GTER40**, eu já alertava que **seu maior inimigo pode ser você**. E a realidade não mudou.

HTTPS://NEXTHOP.SOLUTIONS

ESTEJA PREPARADO

Problemas acontecem, e vão continuar acontecendo...

Pra começar a realmente se preparar para sobreviver ao cenário atual, você deve entender que:

- Falhas de segurança em firmwares não são novidade. E eles vão acontecer... seja hoje, amanhã ou depois.
- Seja "chato" com gerência, ter acl de controle lá na ponta não é suficiente.
- Você não tem como impedir seu cliente de comprar dispositivos de origem/software duvidosos, mas tem obrigação de cuidar da sua rede.
- Estude e descubra que SNMP não é suficiente.
- Tenha soluções de análise e, preferencialmente, de ações automatizadas.

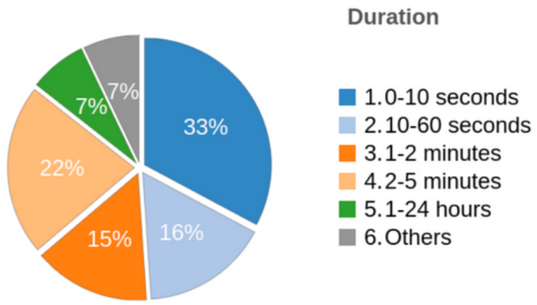
E a mais importante: **Cuide do seu lixo**.

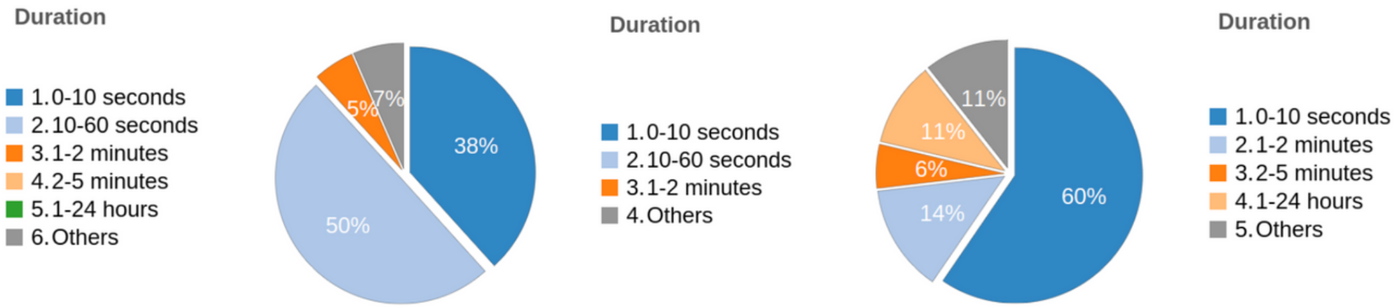
HTTPS://NEXTHOP.SOLUTIONS

2025, O QUE FAZER?

Técnicas e Atitudes que podem salvar sua rede

Estatisticamente, na atualidade, a maioria das redes dos ISPs sofrem muito mais com **ataques rápidos**, com milhões de pacotes do segundo, que não inundam ou extrapolam sua capacidade de banda, mas que geram inúmeros problemas dentro das redes, do que com ataques volumétricos.





HTTPS://NEXTHOP.SOLUTIONS

2025, O QUE FAZER?

Técnicas e Atitudes que podem salvar sua rede

Para esses casos, procure por sistemas que tenham suporte a flowspec e tenha certeza que seu hardware de borda tenha suporte e seja eficiente em sua aplicação.

Wanguard e Huawei é uma boa dobradinha.

Juntos, e bem configurados, eles são capazes de responder e criar uma grande quantidade de regras de proteção em frações de segundos e proteger sua infra.

Isso é parte da solução, e com as licenças adequadas você consegue evitar a virada pra nuvem de mitigação em até **80% dos casos**.

ANTES DE CONTINUAR...

Não se esqueça do básico

- Garanta que sua rede não tenha loops de roteamento
- Aplique técnicas anti-spoofing (https://bcp.nic.br/antispoofing)
- Homologue sua rede no MANRS (https://manrs.org/)
- Use dns próprio, com suporte total a IPv6
- Garanta que você tem a habilidade de desviar todo seu upload de forma fácil
- Tenha um bom sistema de observabilidade em tempo real
- Implemente RPKI (completo)
- Escolha uma boa nuvem de mitigação

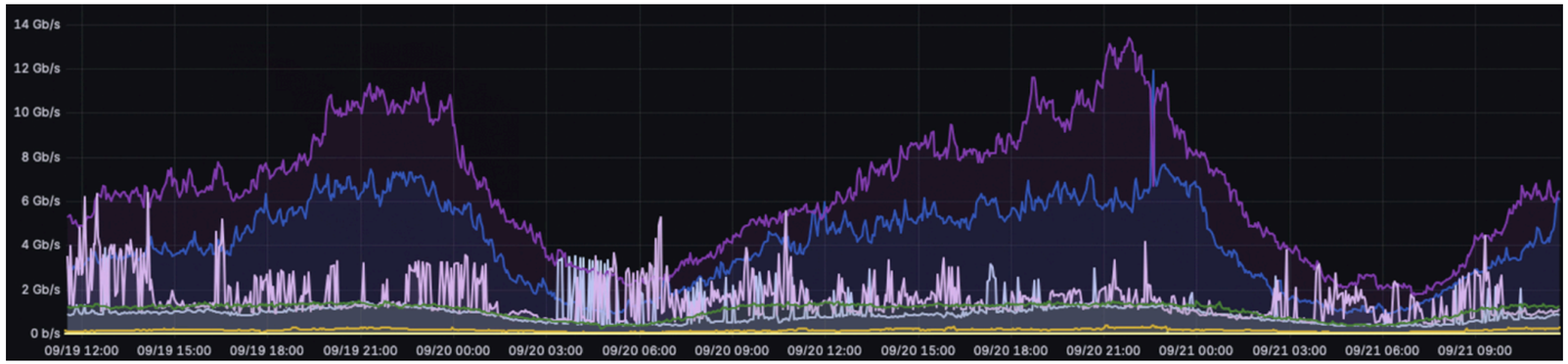
HTTPS://NEXTHOP.SOLUTIONS

PROBLEMAS RECENTES

CPEs Infectadas expõe um problema maior...

Recentemente tivemos uma onda conjunta de CPEs infectadas, TvBOX piratas infectados, DVRs, Câmeras e diversos outros tipos de dispositivos participando de botnets e expondo um problema ainda maior para os ISPs.

Durante muito tempo, a grande maioria dos ISPs se preocupou apenas em o que fazer quando **receber** um ataque. E, mais do que nunca, fica exposto um novo desafio... **como não ser parte do problema, o atacante...**



HTTPS://NEXTHOP.SOLUTIONS

A REALIDADE

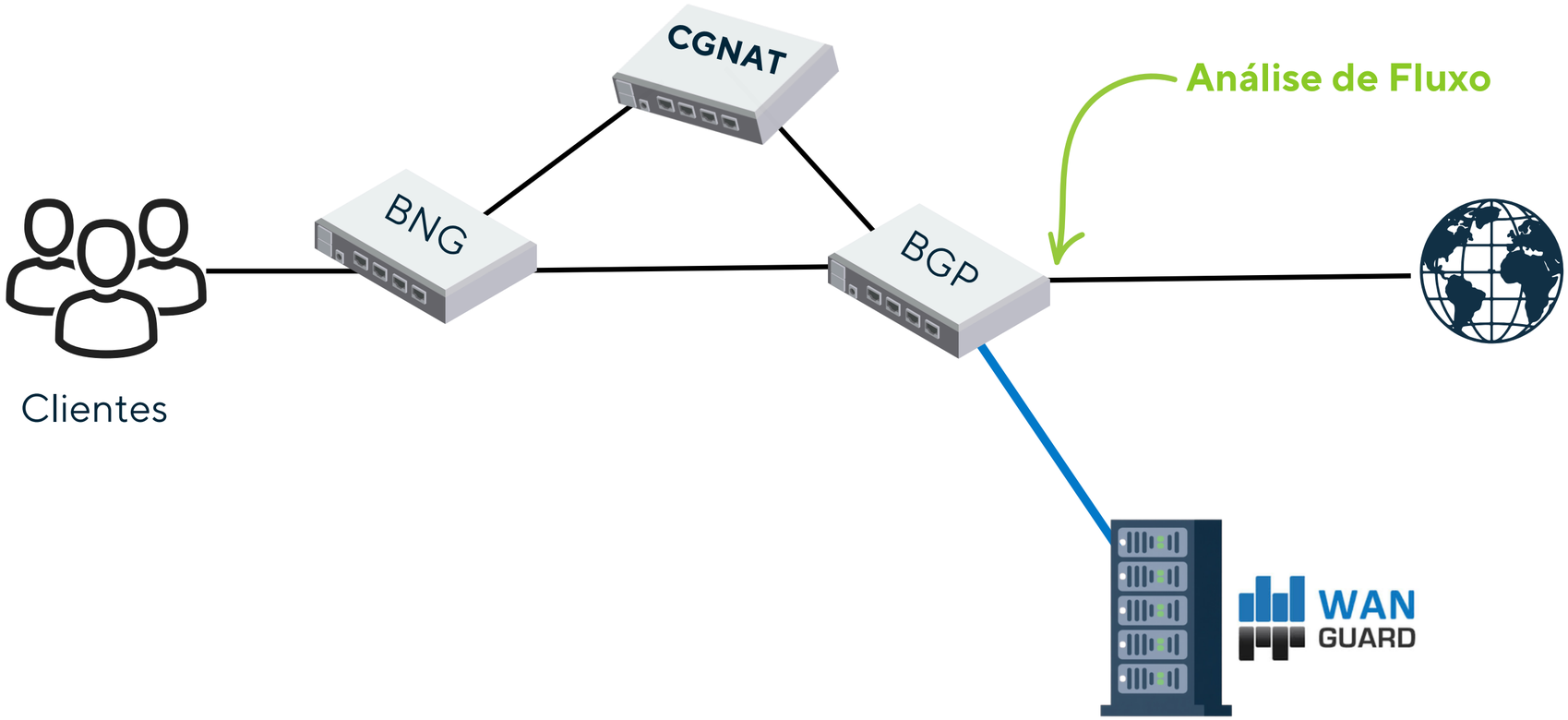
Algumas verdades nem sempre são agradáveis de ouvir...

- Se todos fizessem o dever de casa, ataques DDOS não existiriam
- Se você não cuida/trata a saída de ataques como trata a entrada, você é parte do problema
- Nuvens de mitigação não fazem milagres, **alguns** efeitos colaterais são normais
- Uma rede que sofre efeitos colaterais é melhor que uma rede parada
- Uma rede sob ataque nunca será "tranquila"
- Um DNS Recursivo externo só será melhor que o seu próprio se ele foi construído/configurado errado, ou arquitetado de forma errada

Mas, você pode diminuir drasticamente os impactos na sua rede com as ações e sistemas certos.

OBSERVANDO O QUE SAI

Cenário Comum nos ISPs

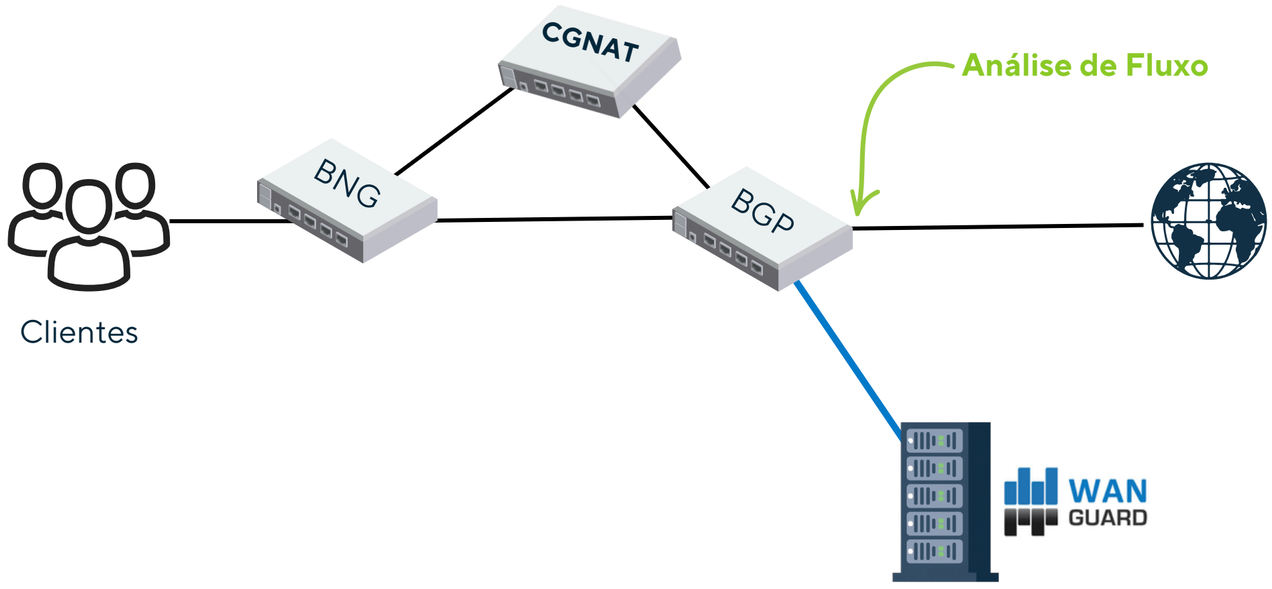


HTTPS://NEXTHOP.SOLUTIONS

OBSERVANDO O QUE SAI

Problemas do cenário convencional

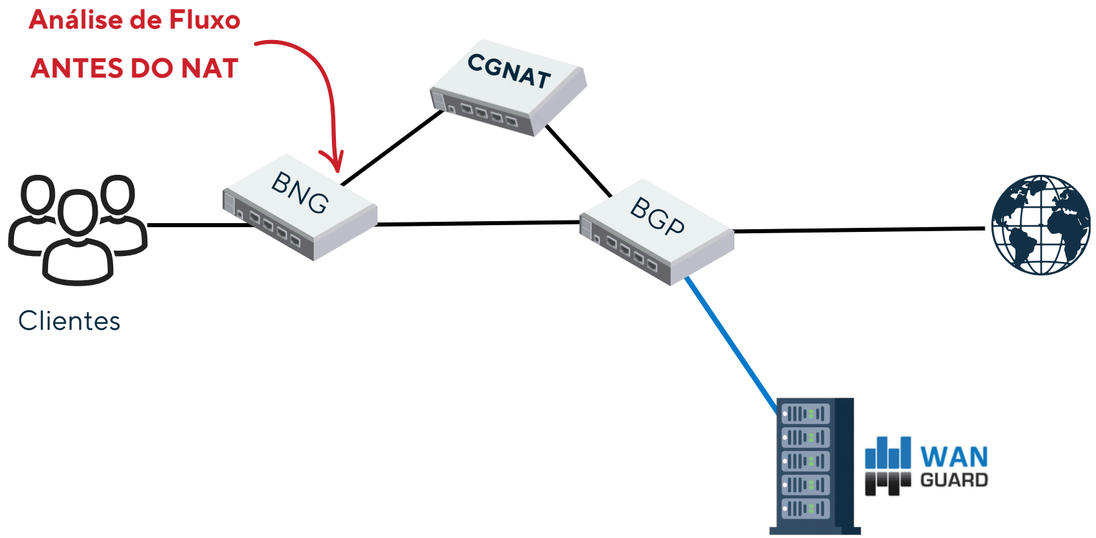
O problema aqui é que o fluxo é analisado após o NAT já ter ocorrido. Assim, ainda que seja possível identificar o "cliente" interno, seria bem mais trabalhoso.



OBSERVANDO O QUE SAI

Problemas do cenário convencional

A forma mais eficiente para conseguir analisar quem dentro da rede está "gerando" ataques, é analisando o tráfego **antes que o NAT aconteça**. Assim você será capaz de obter exatamente o IP privado, bastando consultar no seu ERP quem é o cliente que está originando os ataques.

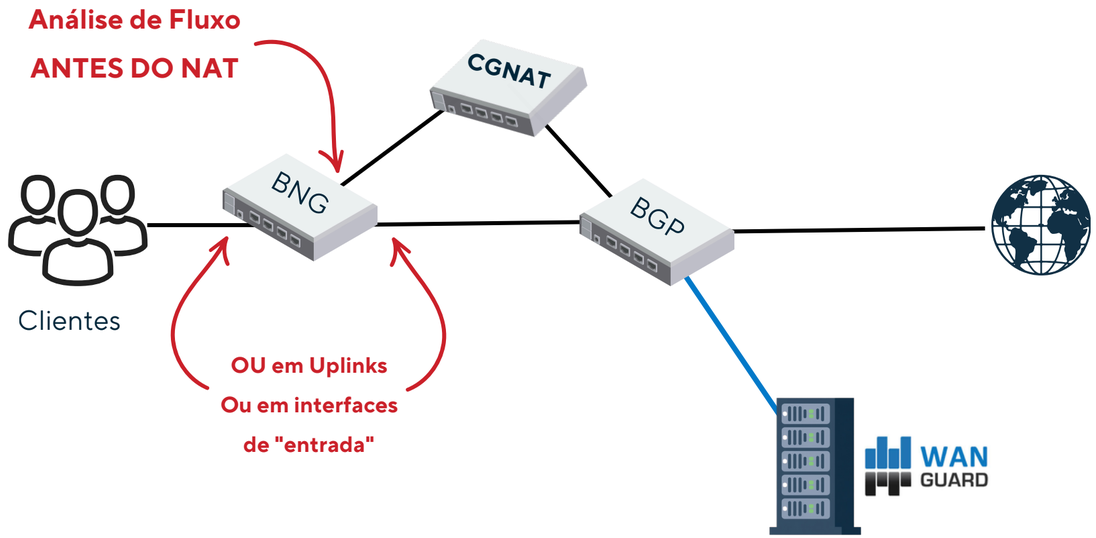


HTTPS://NEXTHOP.SOLUTIONS

OBSERVANDO O QUE SAI

Problemas do cenário convencional

A forma mais eficiente para conseguir analisar quem dentro da rede está "gerando" ataques, é analisando o tráfego **antes que o NAT aconteça**. Assim você será capaz de obter exatamente o IP privado, bastando consultar no seu ERP quem é o cliente que está originando os ataques.



HTTPS://NEXTHOP.SOLUTIONS

QUAL SOFTWARE USAR

Sem gastar com licenças

Existem soluções opensource e/ou disponibilizados de forma gratuita, que servem como uma das soluções alternativas aos softwares "comuns" e que podem lhe dar a observabilidade e informações necessárias para que você tenha uma visão completa sobre o que acontece na sua rede.

NEXTHOP SOLUTIONS

HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Instalação

A stack completa, você consegue rodar com apenas 3 comandos, e o repositório possui instruções mais detalhadas no README.

git clone git@github.com:nexthopsolutions/nxt-netflow-stack.git

cd nxt-netflow-stack && cp env.example .env

docker compose up -d

Ou docker-compose up -d (dependendo da versão).

STACK NETFLOW

Instalação

Depois basta enviar os flows, a partir do roteador desejado para a porta configurada no .**env** e você já será capaz de acessar a stack.

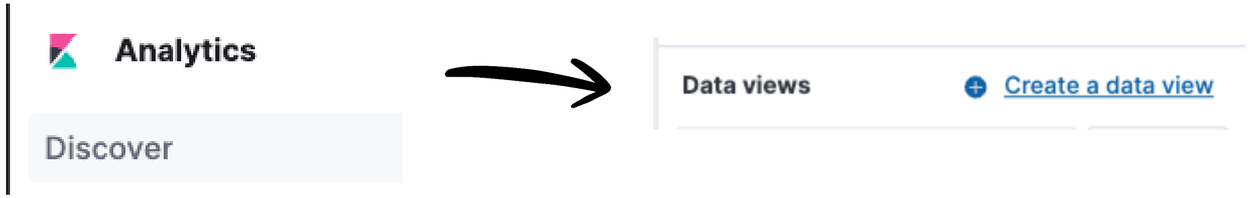
Para acesso ao kibana, acesse a url **http://IP-DA-MÁQUINA:5601**

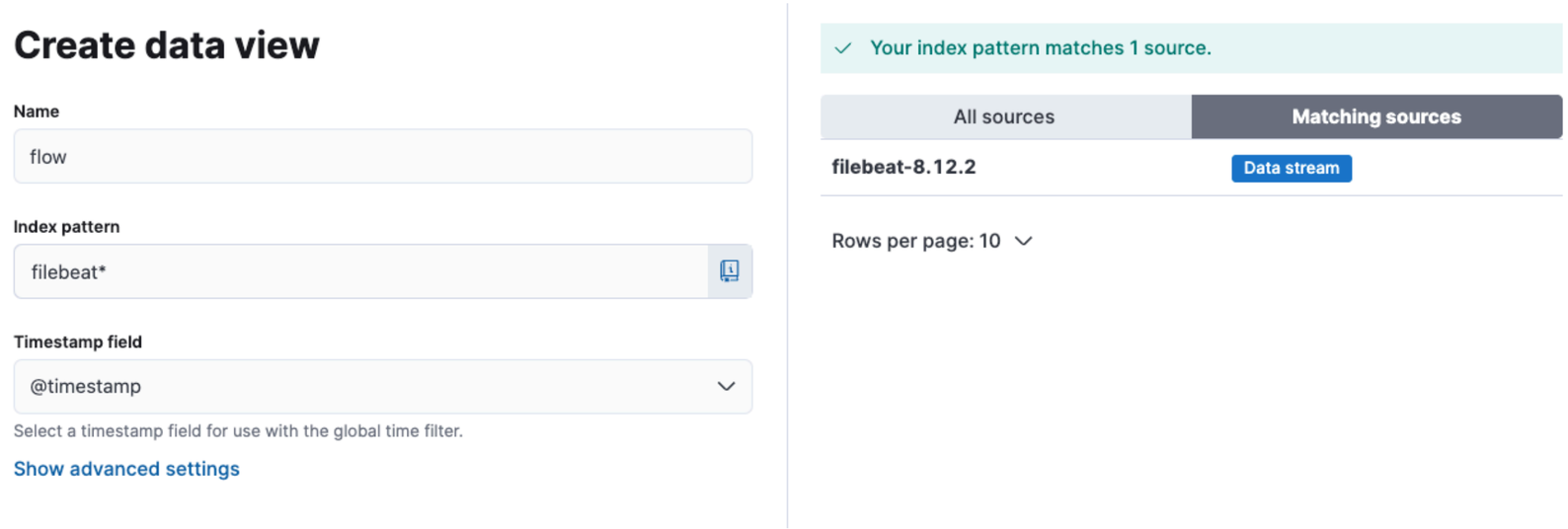
Usuário: elastic
Senha: definida no .env

STACK NETFLOW

Configuração

No menu analitcs → discovery, crie um novo data view com nome **netflow**, e com pattern dando "match" no filebeat.

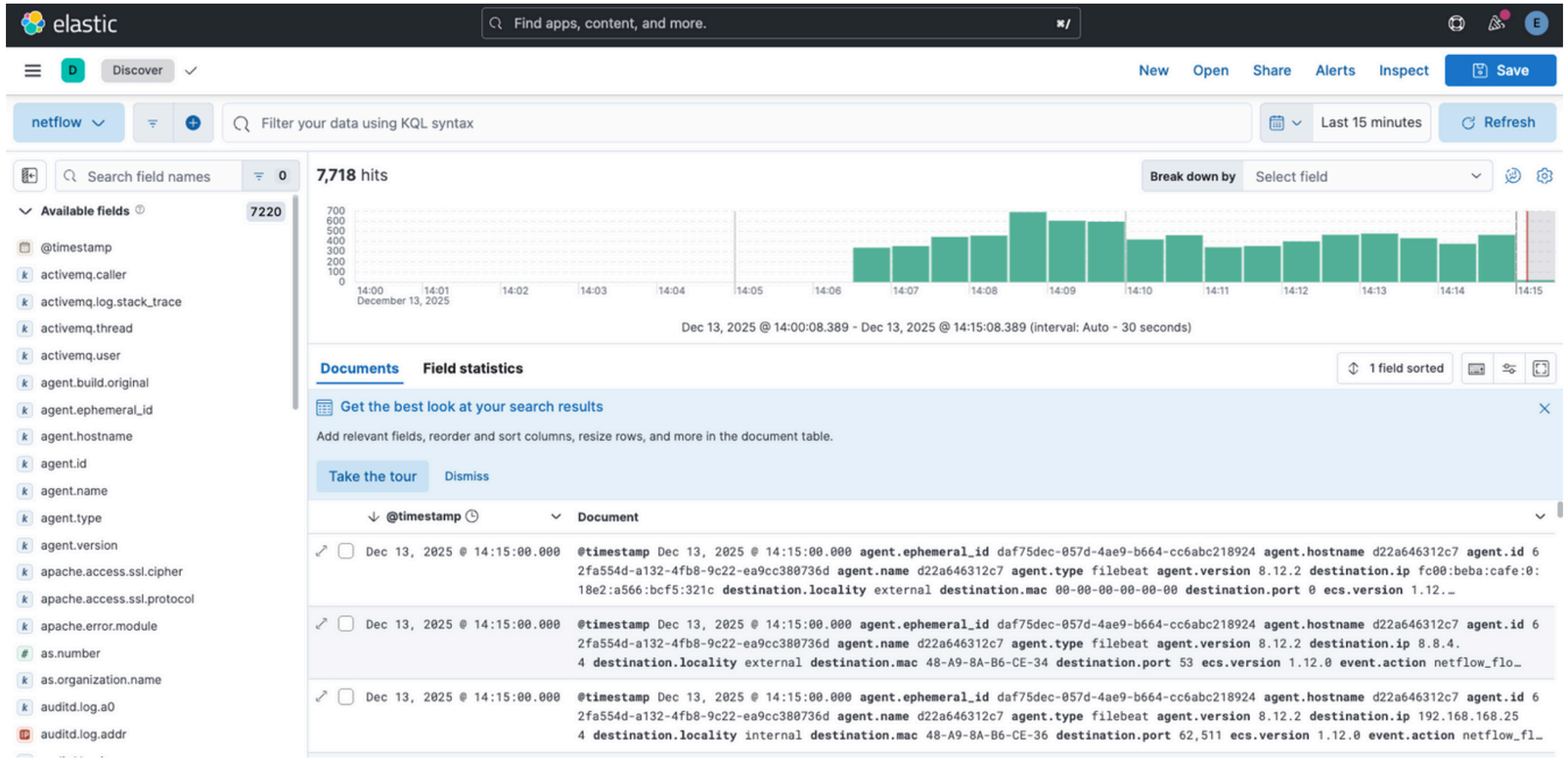




STACK NETFLOW

Configuração

Assim você já conseguirá ver o fluxos sendo recebidos:



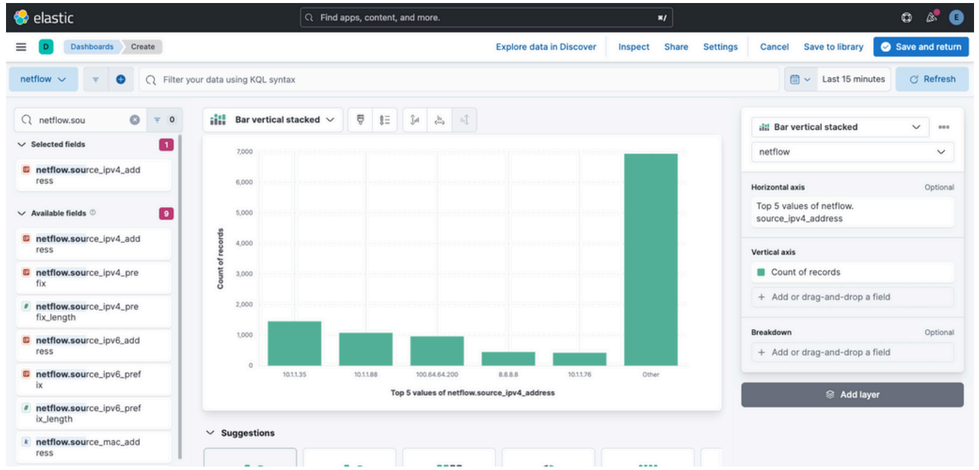
HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

Você pode criar **dashboards** dentro do próprio kibana, mas a stack já oferece um **grafana** e templates para ele integrados.

Você pode acessar o grafana da stack, na porta **3000** com usuário **admin** e a senha definida no **.env**

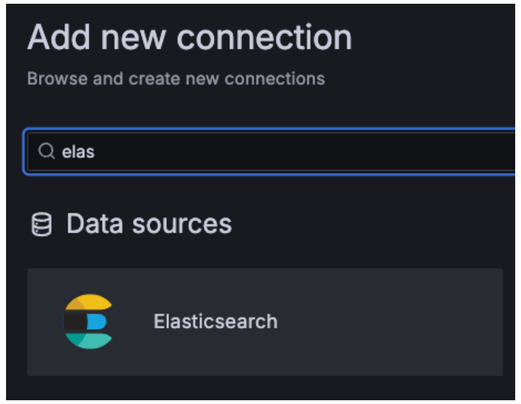


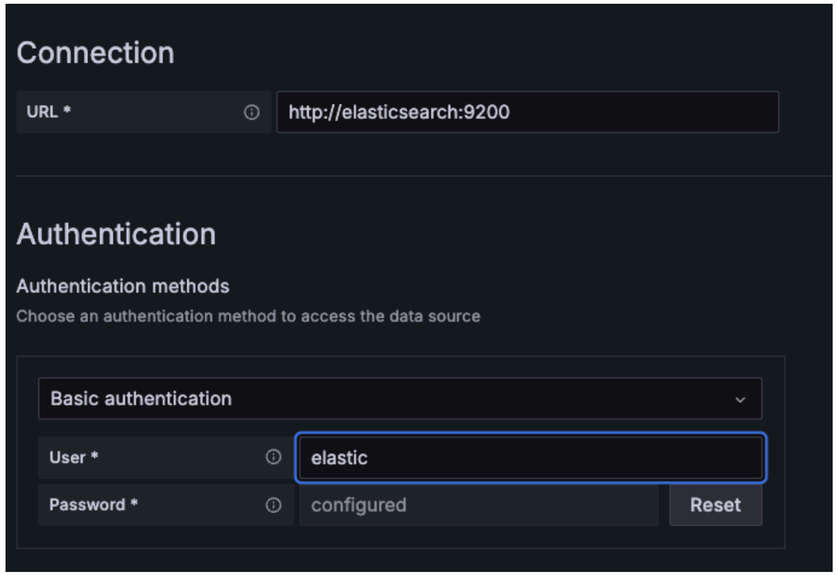
HTTPS://NEXTHOP.SOLUTIONS

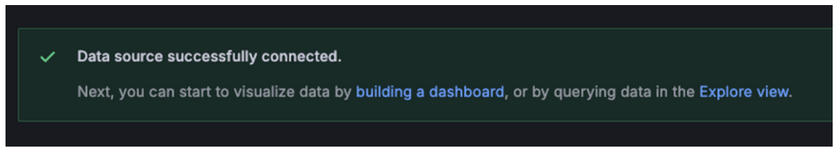
STACK NETFLOW

Configuração

No grafana, em **Connections** → **Add new connection**, procure por **elasticksearch** e adicione um novo **datasource**.





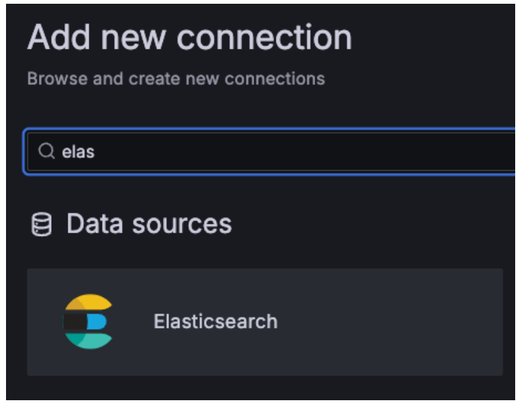


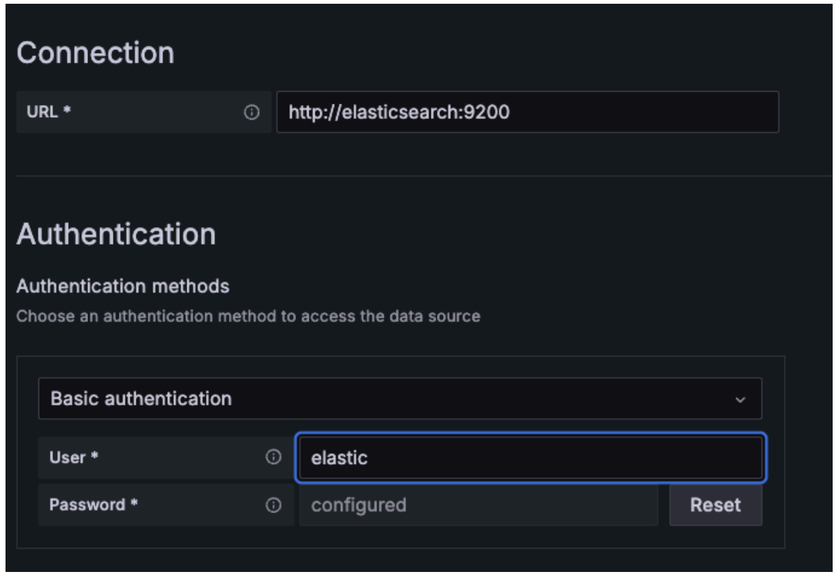
HTTPS://NEXTHOP.SOLUTIONS

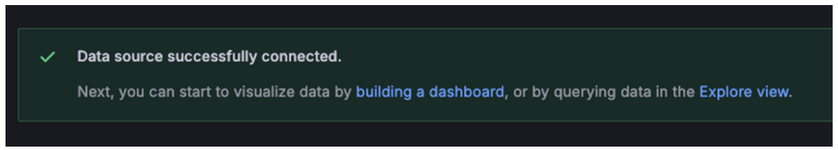
STACK NETFLOW

Configuração

No grafana, em **Connections** → **Add new connection**, procure por **elasticksearch** e adicione um novo **datasource**.





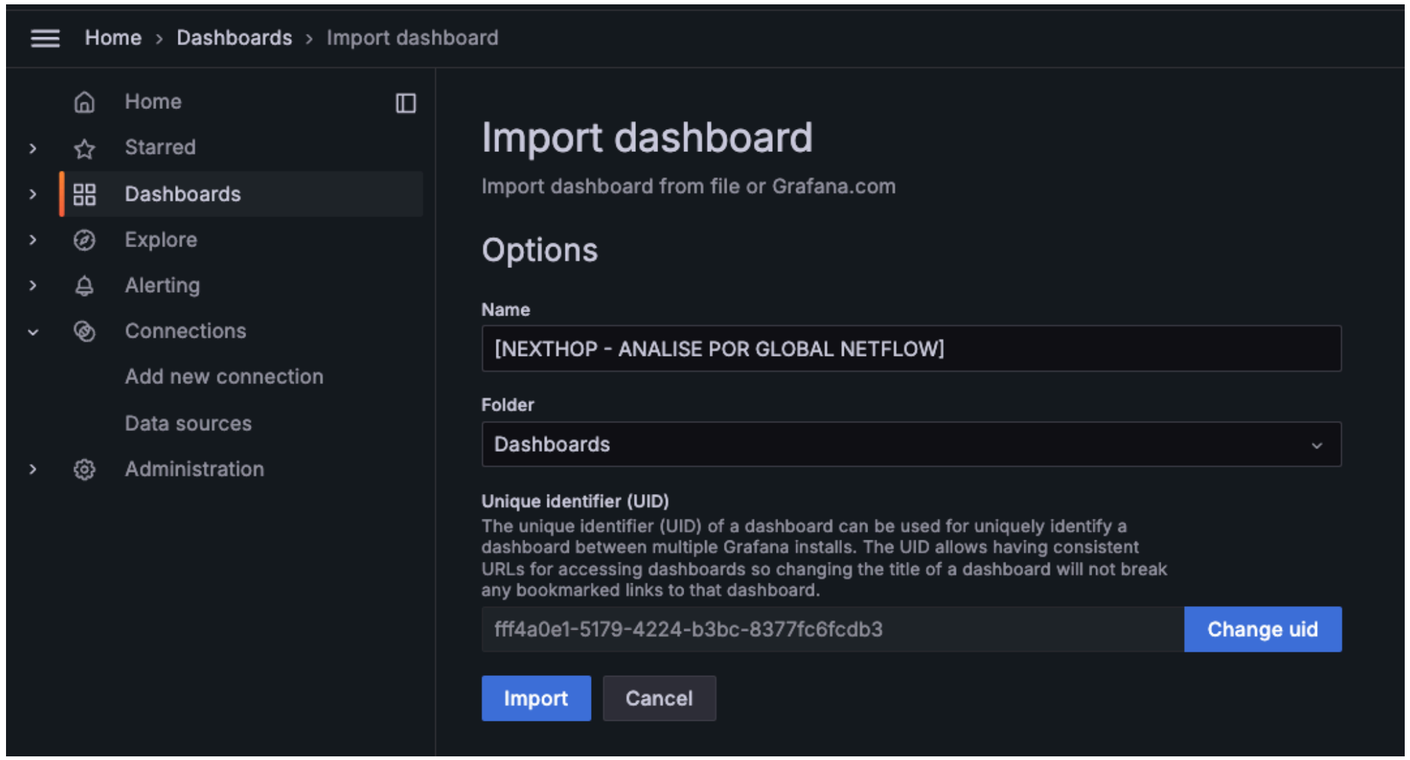


HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

Depois basta importar a dashboard do repositório e ajustá-la para o datasource atual.

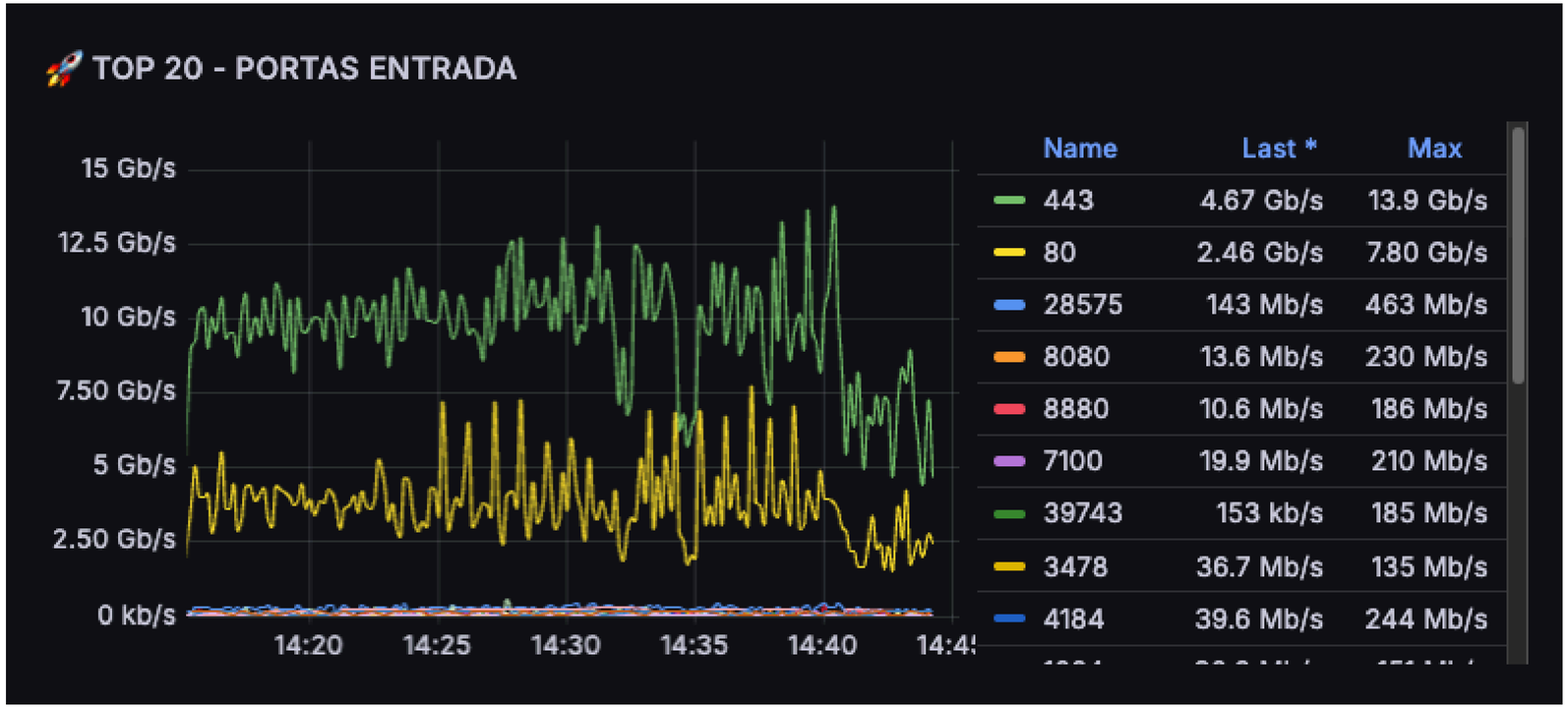


HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

E pronto, você já terá uma visualização **real** e **muito mais completa** da sua rede.

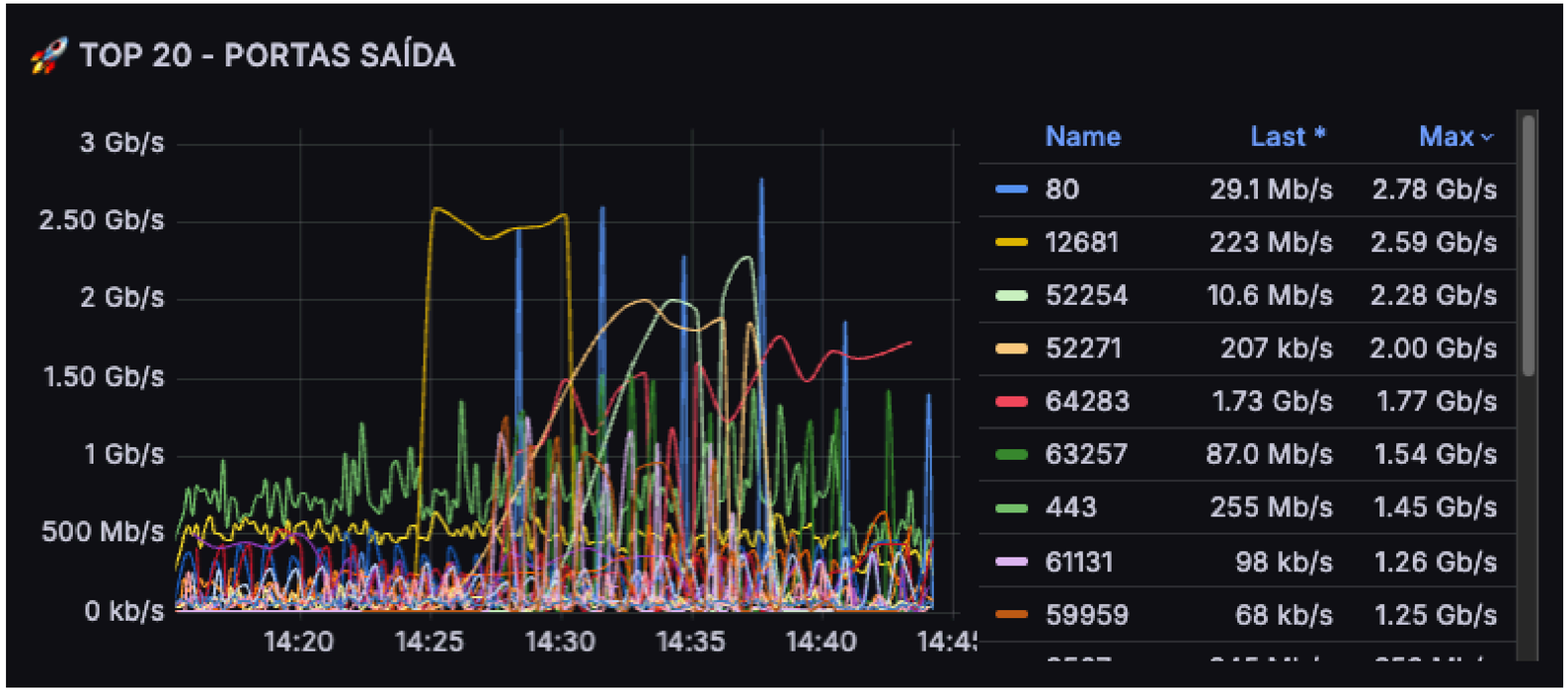


HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

E pronto, você já terá uma visualização **real** e **muito mais completa** da sua rede.

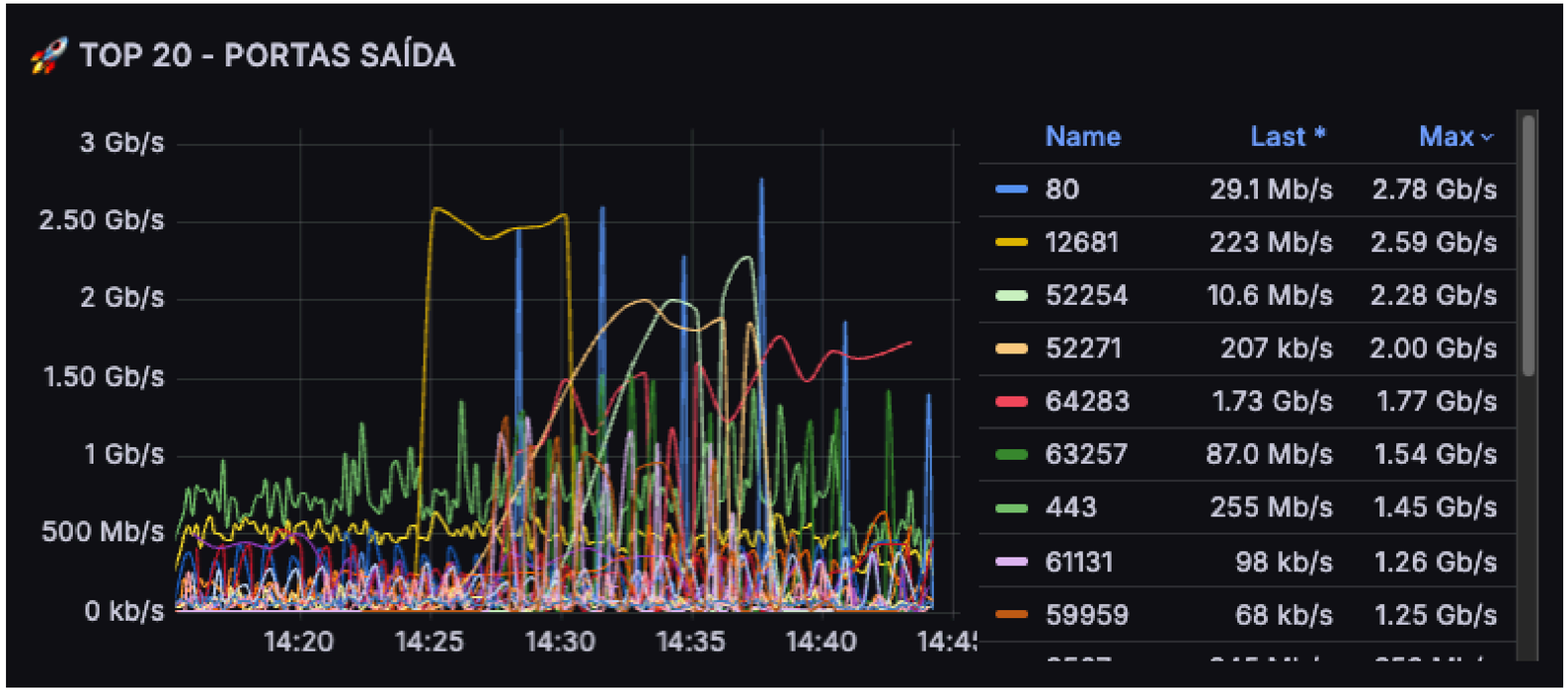


HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

E pronto, você já terá uma visualização **real** e **muito mais completa** da sua rede.

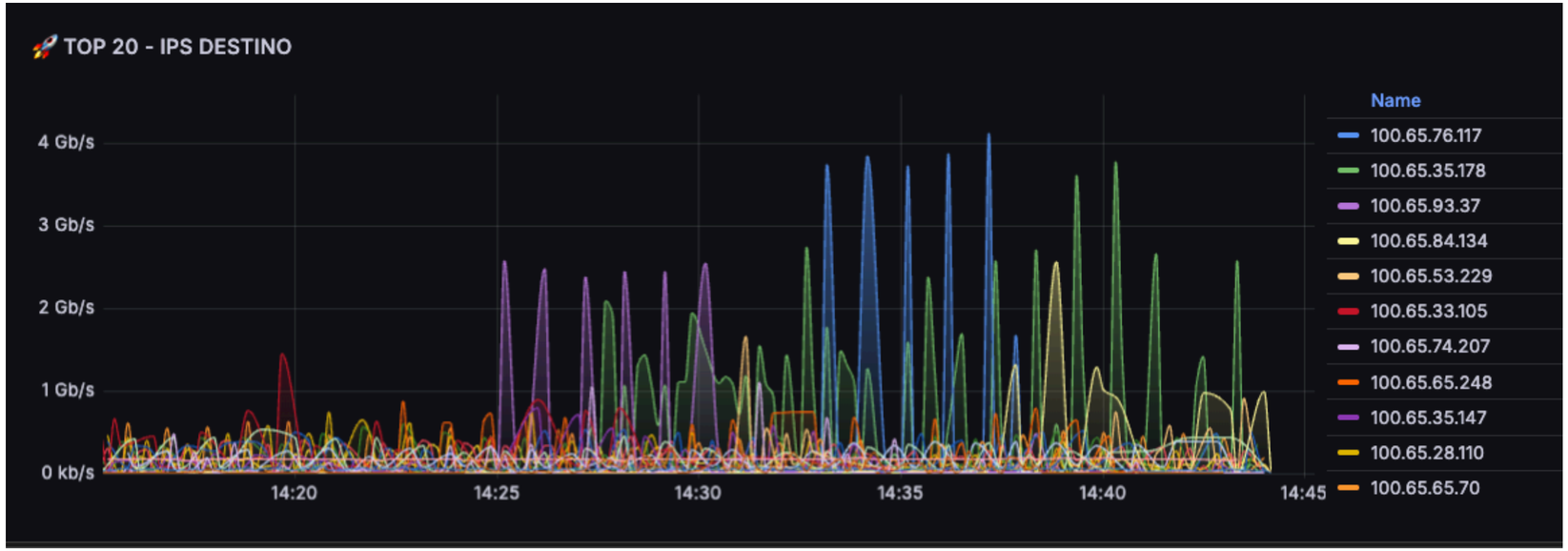


HTTPS://NEXTHOP.SOLUTIONS

STACK NETFLOW

Configuração

E será capaz de identificar, com uma precisão maior, os **IPS PRIVADOS** e **PÚBLICOS** que originam ataques de dentro da sua rede.



HTTPS://NEXTHOP.SOLUTIONS

E DEPOIS?

Com atacantes identificados, o que fazer?

TOME UMA AÇÃO!

Isso é o mais importante.

As ações variam de acordo com a realidade de cada ISP/Rede, alguns tentam identificar dentro da casa do assinante qual é o dispositivo remotamente, outros levam uma routerboard em bridge e ligam direto na cpe do cliente pra identificar dentro da rede do cliente, qual dispositivo está originando os ataques... e outros notificam o cliente dando um prazo pra resolver sob pena de ter seu acesso suspenso.

Independente de qual seja, tome uma ação! E lembre-se: **QUEM ATACA CHAMA ATAQUE**.

E NA BORDA?

Alternativas para reduzir impactos...

Lembre-se: **LINK PROTEGIDO NÃO É NUVEM DE MITIGAÇÃO**.

E um dos grandes problemas das implementações convencionais que vemos, de sistemas como **wanguard** (por exemplo), é que a licença "sensor" permite o flowspec de maneira tradicional (e limitada), ou seja:

O **flowspec atua apenas no destino**. E isso pode te trazer efeitos colaterais que muitas vezes podem fazer você ter uma visão que a implementação **mais atrapalha do que ajuda**.

HTTPS://NEXTHOP.SOLUTIONS

E NA BORDA?

Alternativas para reduzir impactos...

Lembre-se: **LINK PROTEGIDO NÃO É NUVEM DE MITIGAÇÃO**.

E um dos grandes problemas das implementações convencionais que vemos, de sistemas como **wanguard** (por exemplo), é que a licença "sensor" permite o flowspec de maneira tradicional (e limitada), ou seja:

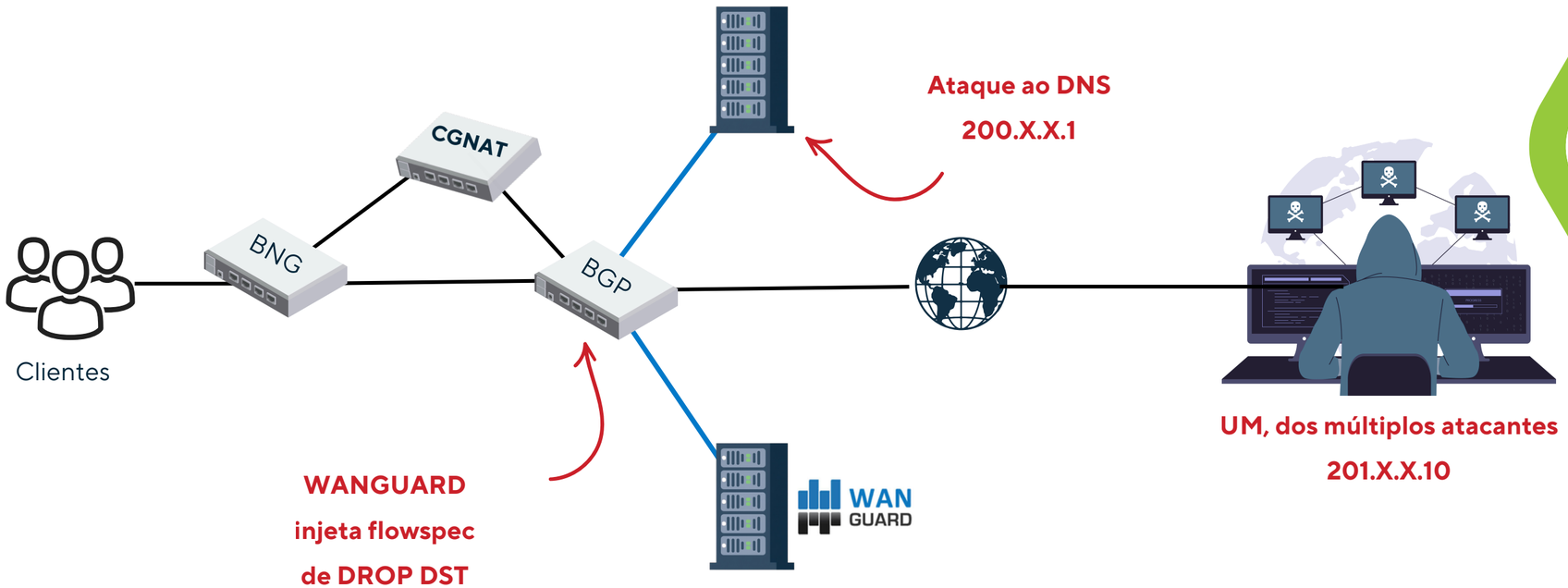
O **flowspec atua apenas no destino**. E isso pode te trazer efeitos colaterais que muitas vezes podem fazer você ter uma visão que a implementação **mais atrapalha do que ajuda**.

HTTPS://NEXTHOP.SOLUTIONS

E NA BORDA?

Alternativas para reduzir impactos...

Exemplo: Um ataque em direção ao seu servidor DNS, pode fazer com que o flowspec atue e literalmente **pare** sua rede.



HTTPS://NEXTHOP.SOLUTIONS

E NA BORDA?

Alternativas para reduzir impactos...

O problema do cenário apresentado, é que todo tráfego (**incluindo o legítimo**) com destino ao seu DNS, seria dropado. O resultado você já sabe....

Uma alternativa que soluciona esse problema e é utilizado por muitas empresas (inclusive de nuvens de mitigação) é a licença **filter** do wanguard. Ela habilita a possibilidade de você realizar filtros de flowspec **por origem**.

Assim, você consegue dropar o tráfego **apenas dos atacantes** e permite que o tráfego legítimo continue fluindo normalmente.

Isso reduz em até 90% os efeitos colaterais para esse tipo de situação dentro da sua rede.

HTTPS://NEXTHOP.SOLUTIONS

E NA BORDA?

Alternativas para reduzir impactos...

Além do mais, você também terá um segundo recurso importante, que está diretamente ligado ao apresentado anteriormente.

Você também conseguirá evitar que um tráfego ORIUNDO da sua rede, seja propagado para fora, sem afetar os demais clientes.

De forma resumida, é como você pode diminuir os impactos que os dispositivos da sua rede, que geram ataques pra fora, tenham tanto impacto.

Isso não resolve o problema, mas melhora significativamente o impacto que sua rede pode causar na "internet" como um todo.

Lembre-se, do outro lado também tem uma vítima.

NEXTHOP SOLUTIONS

HTTPS://NEXTHOP.SOLUTIONS

E NA BORDA?

Alternativas para reduzir impactos...

Além do mais, você também terá um segundo recurso importante, que está diretamente ligado ao apresentado anteriormente.

Você também conseguirá evitar que um tráfego ORIUNDO da sua rede, seja propagado para fora, sem afetar os demais clientes.

De forma resumida, é como você pode diminuir os impactos que os dispositivos da sua rede, que geram ataques pra fora, tenham tanto impacto.

Isso não resolve o problema, mas melhora significativamente o impacto que sua rede pode causar na "internet" como um todo.

Lembre-se, do outro lado também tem uma vítima.

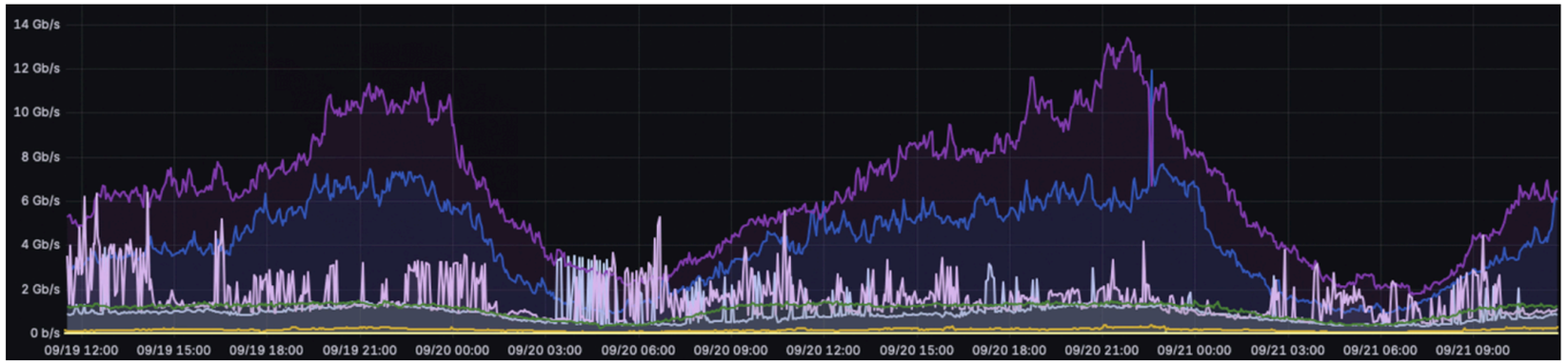
NEXTHOP SOLUTIONS

HTTPS://NEXTHOP.SOLUTIONS

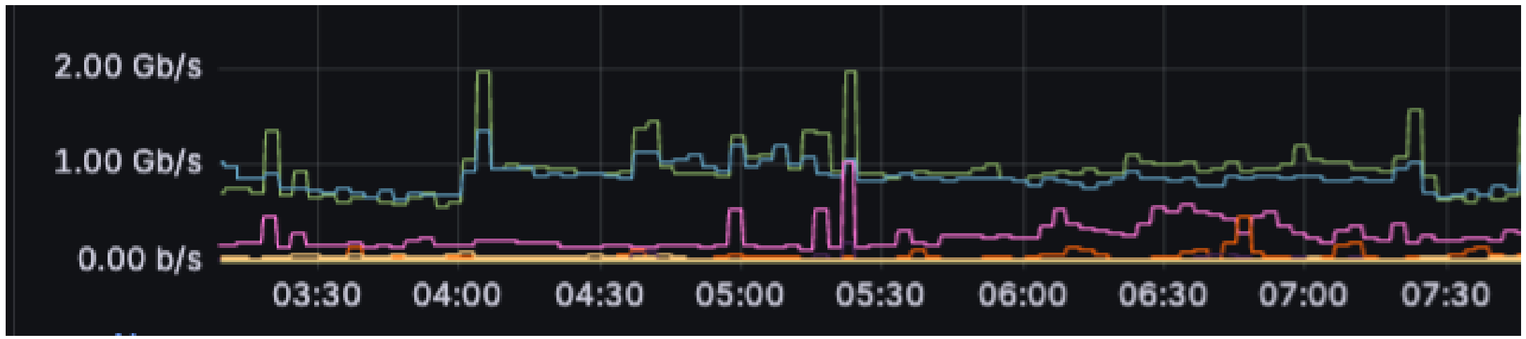
E NA BORDA?

Alternativas para reduzir impactos...

E aí você sai disso:



Pra isso:



HTTPS://NEXTHOP.SOLUTIONS

DÚVIDAS

NETWORK EDUCATION

10 ANOS

A SUA ESCOLA DE TELECOM

Agradecimentos especiais, ao amigo Rubens Kühl:

.

Rubens foi um amigo e grande incentivador. Razão pela qual submeti minha primeira palestra na GTER há mais de 10 anos.

Teve fundamental importância em minha jornada e tem minha eterna gratidão.

Obrigado, amigo!

nic.br cgi.br

E claro, a toda equipe do Nic.BR, CGI.BR e a toda comunidade técnica que nos apoia, prestigia e contribui para uma internet melhor.

nic.br cgi.br

Obrigado

elizandropacheco

elizandropacheco

elizandropacheco