



angolacables

deepconnection



# O que é um DoS/DDoS

DoS/DDoS é um ataque cibernético no qual o agressor procura tornar uma máquina ou recurso de rede indisponível para seus usuários pretendidos, interrompendo temporariamente ou indefinidamente os respectivos sistemas.

## DoS Attack

Único Sistema



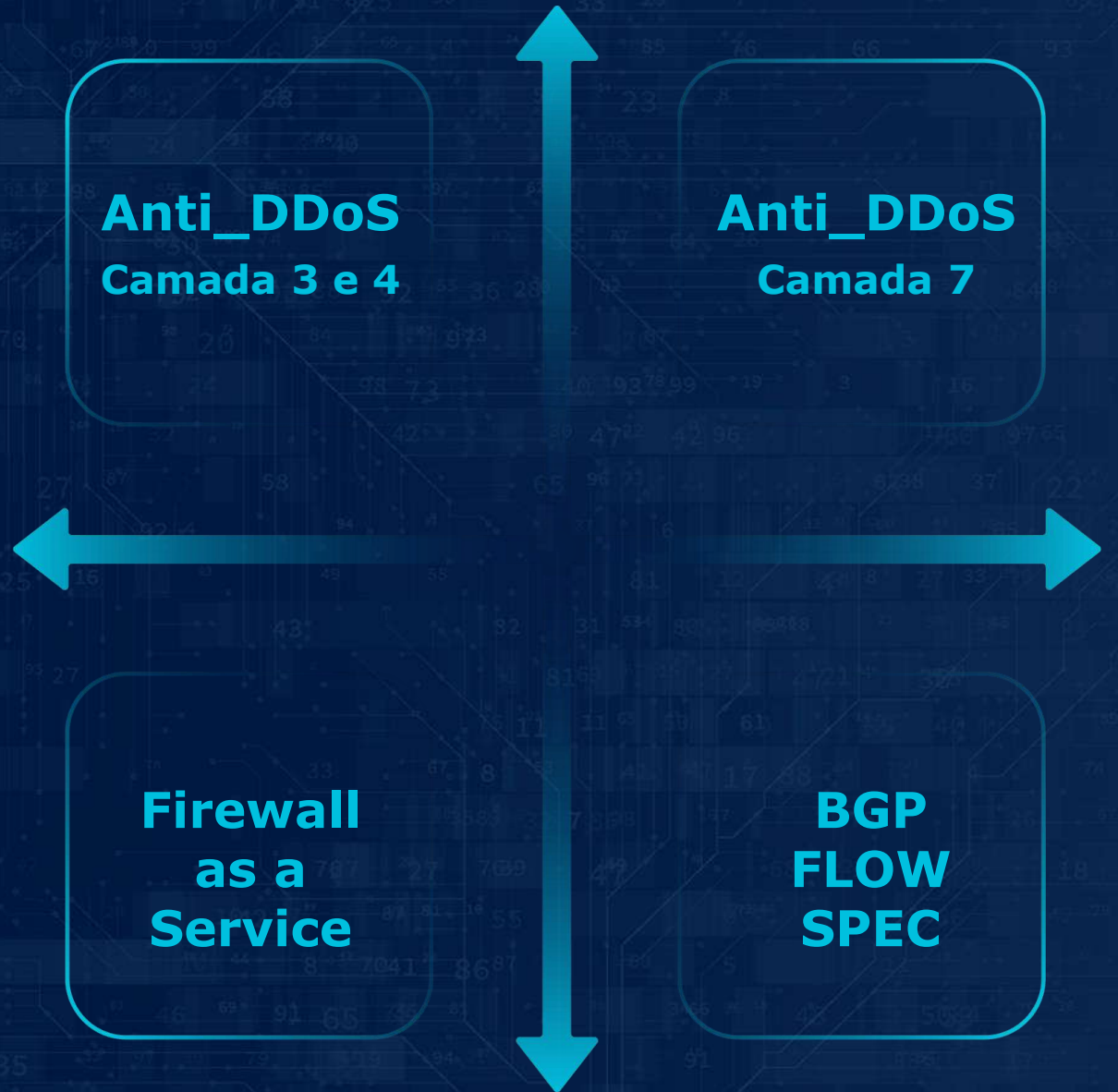
Vítima

## DDoS Attack

Múltiplos sistemas



Vítimas



**Anti\_DDoS**  
**Camada 3 e 4**

**Anti\_DDoS**  
**Camada 7**

**Firewall**  
**as a**  
**Service**

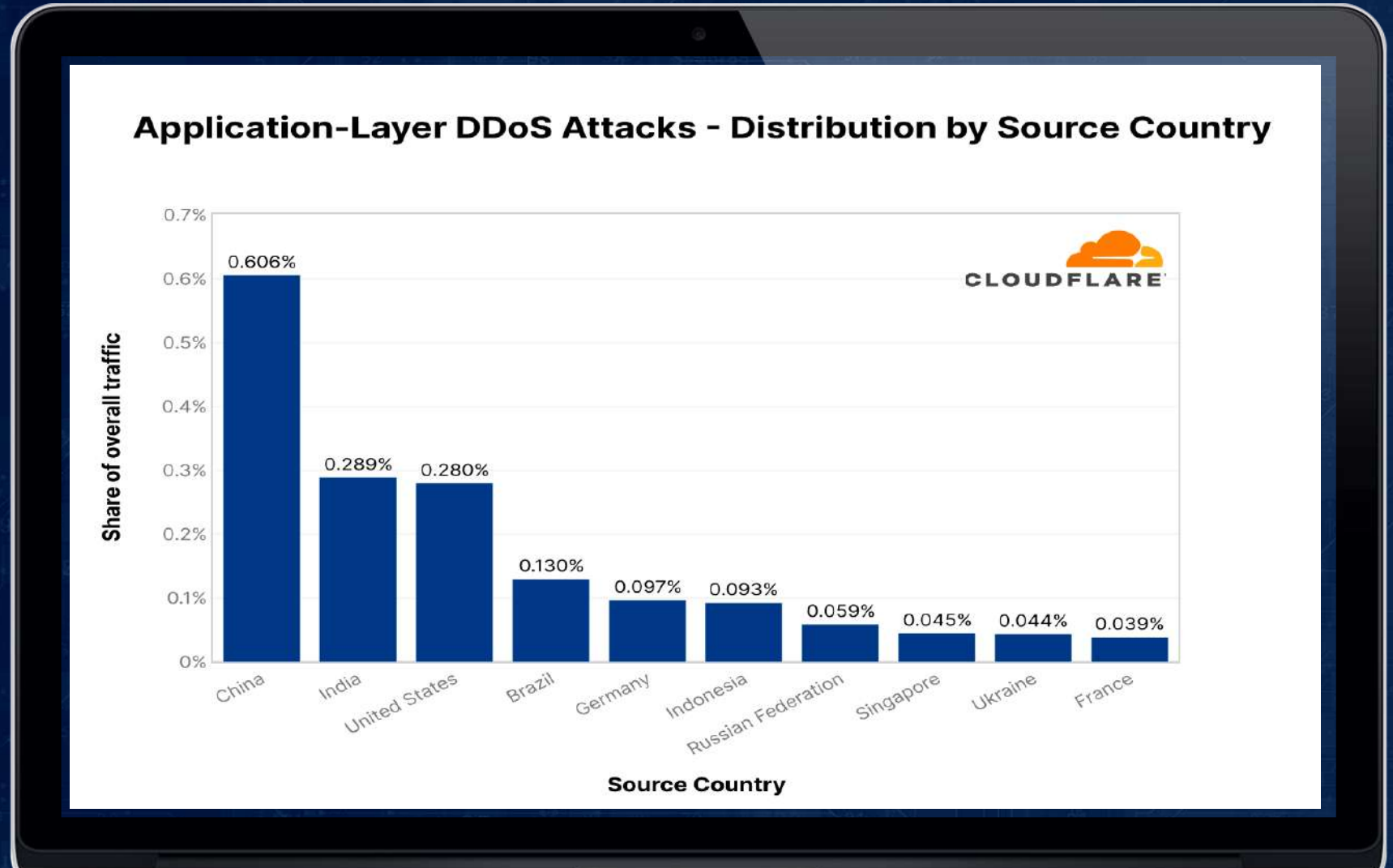
**BGP**  
**FLOW**  
**SPEC**

# Angola Cables no Q3 2022 registrou crescimento de até 307% no volume de ataques contra provedoras de internet do Brasil



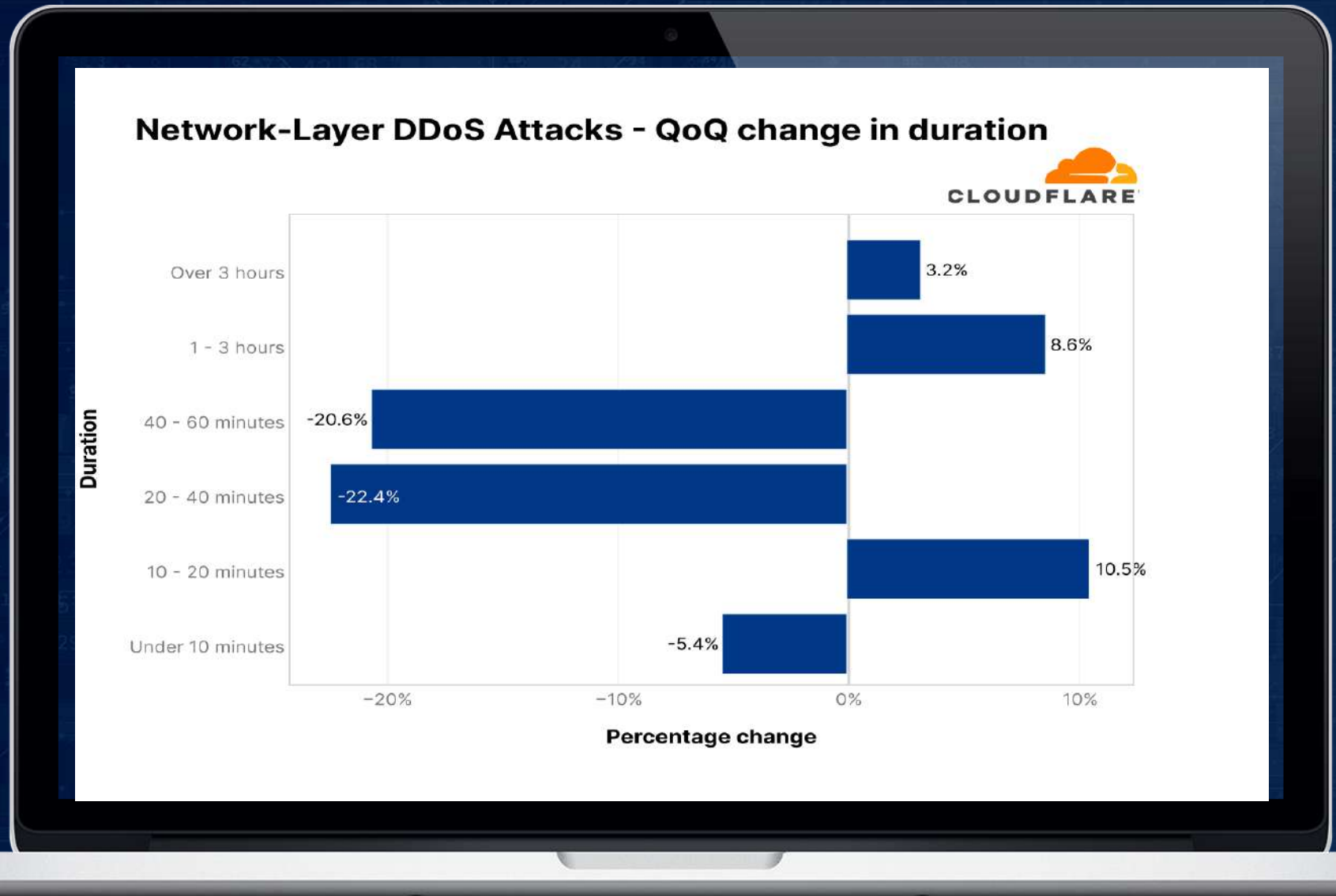
# Tráfego de ataques DDoS na camada de aplicação por país de origem

Depois da Índia, as principais fontes foram os **EUA** e o **Brasil**.

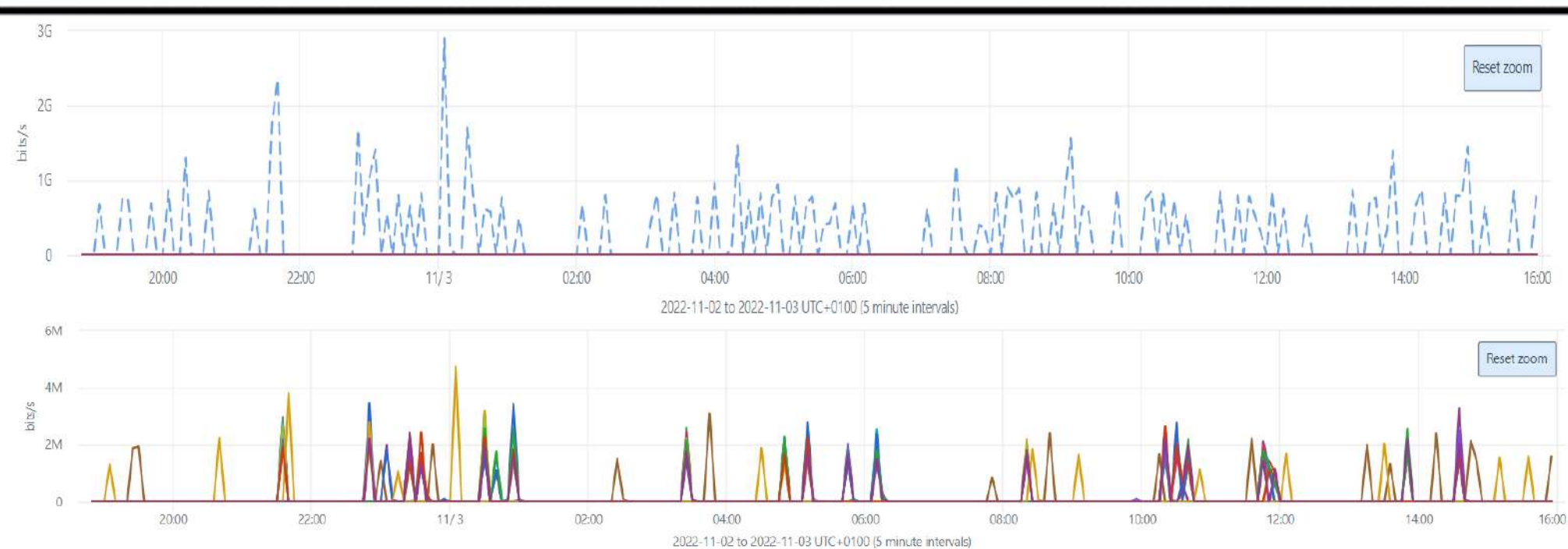


# Mudanças em duração de ataques **Importância e Impacto**

Mudanças em duração de ataque seguido de pouca volumetria visam bypass sistemas de detecção



# Evolução do ataque L3/L4 DDoS Multivector



Destination IP/CIDR	Source Service (Port+Proto)	Average Unique Src IPs	Max Unique Src IPs	Average Kbits/s	Max Kbits/s	Last Datapoint Kbits/s
Total <span>Overlay</span>		2,733	21,849	294.025.17	2,895,286.66	841,671.24
/32	snmp (161/udp)	<1 (0%)	19	106.41 (0.04%)	2,662.15	0.00 (0.00%)
/32	0 (0/udp)	1 (0%)	34	110.85 (0.04%)	3,323.09	0.00 (0.00%)
/32	snmp (161/udp)	<1 (0%)	18	120.21 (0.04%)	2,448.27	0.00 (0.00%)

# Sofrendo Ataque **DDoS** ?

## O que fazer ?



• Deteção



• Desvio



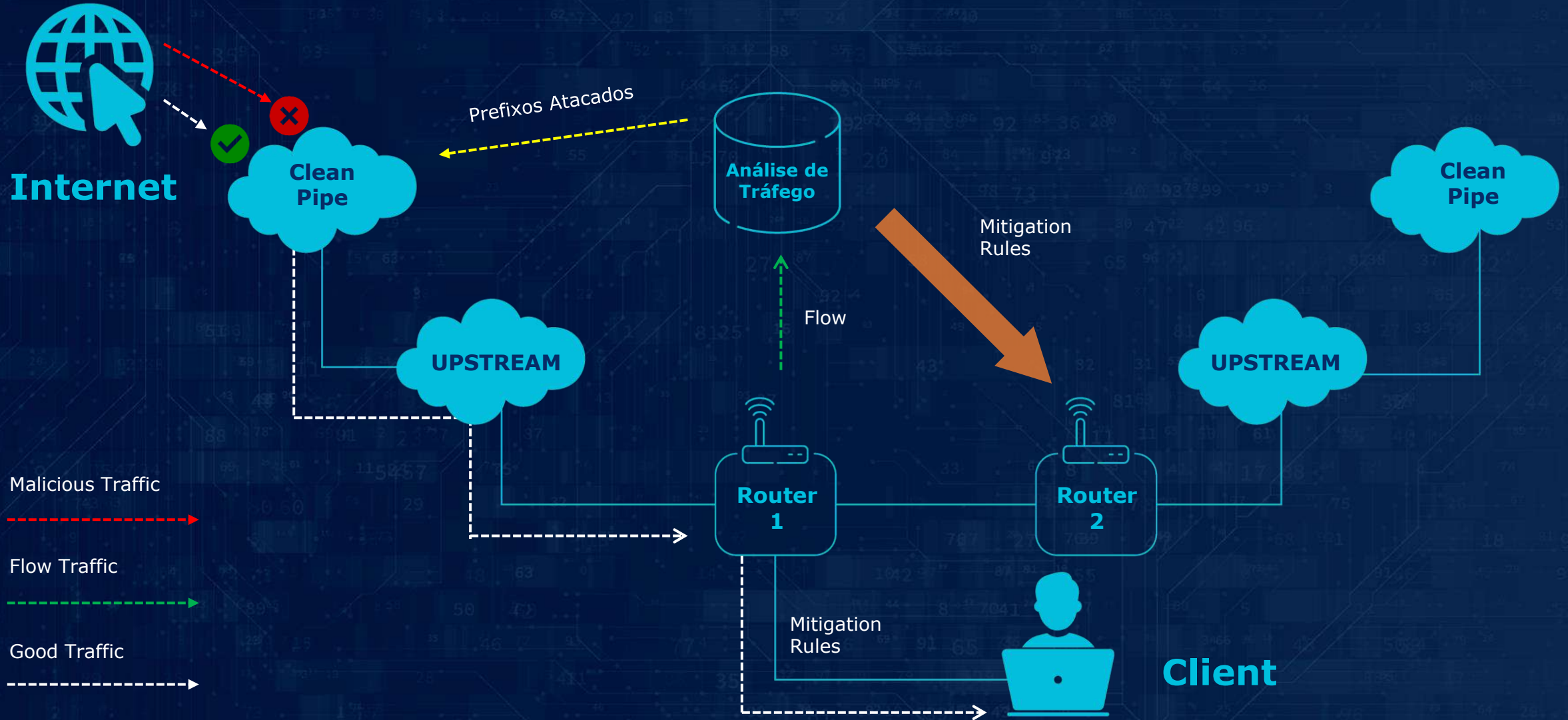
• Filtro



• Analise



# Sistema Integrado de proteção – Angola Cables

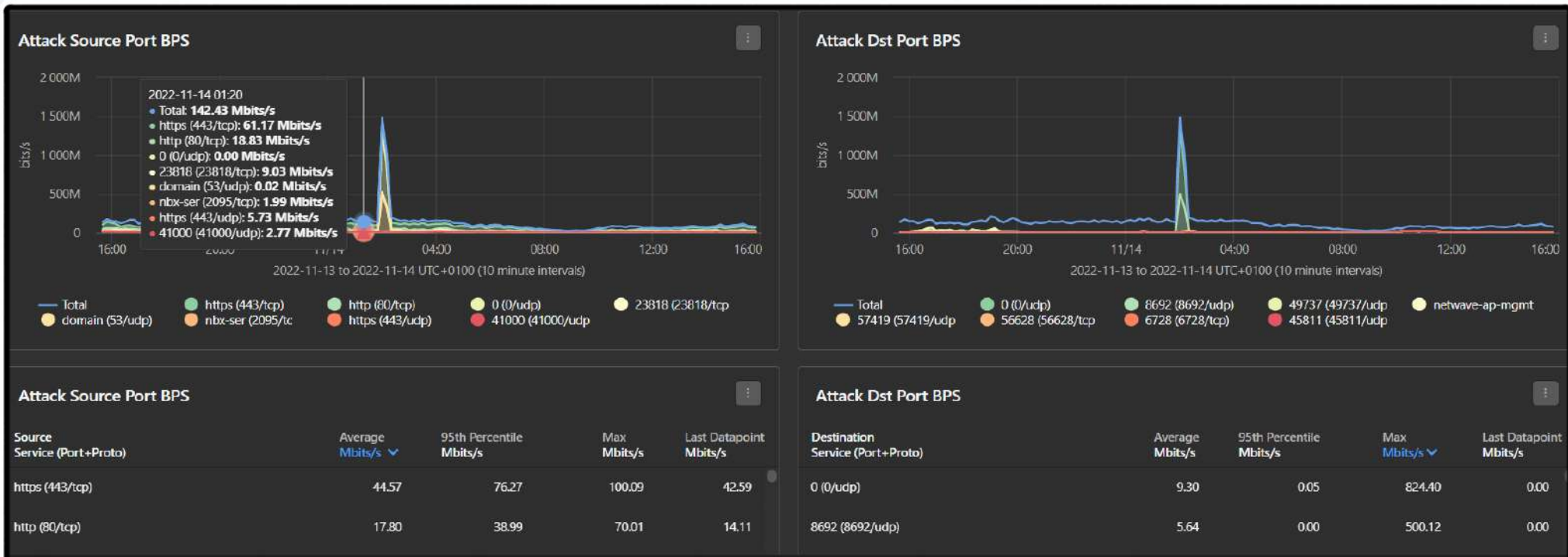


# Angola Cables

## Kentik + Cloudflare

### Benefícios

- ✓ +172 Tbps capacidade em cloud
- ✓ Mitigação até Camada 7
- ✓ Detecção + mitigação <3 segundos
- ✓ Portal de Acesso Personalizado
- ✓ Análise avançada em tempo real
- ✓ Autonomia de envio de regras de mitigação flowspec



# Angola Cables Parcerias

## Kentik + Cloudflare

A Cloudflare foi reconhecida como Líder no Relatório GigaOm Radar 2022 para proteção contra DDoS. O relatório avaliou nove fornecedores diferentes e a Cloudflare foi classificada como a mais alta no geral.

<https://www.cloudflare.com/pt-br/gigaom-radar-ddos-protection/>

Kentik Protect é a solução de detecção de anomalias de rede e DDoS mais precisa do setor, oferecendo ganhos de precisão comprovados em campo de 30% no reconhecimento de ataques

<https://www.kentik.com/resources/kentik-protect-ddos-detection-and-defense/>



angolacables

deepconnection

**Obrigado.**



[angolacables.com](http://angolacables.com)