Boas práticas de rede para mitigação de ataques DDoS

Por Daniel Damito

O que a Sage Networks faz

Empresa especializada em:

- Serviços de Redes
  - Foco em roteamento, performance e otimização de recursos.
- Anti DDoS
  - Detecção automática, Mitigação em Nuvem e tudo o que for necessário para mitigar qualquer ataque.

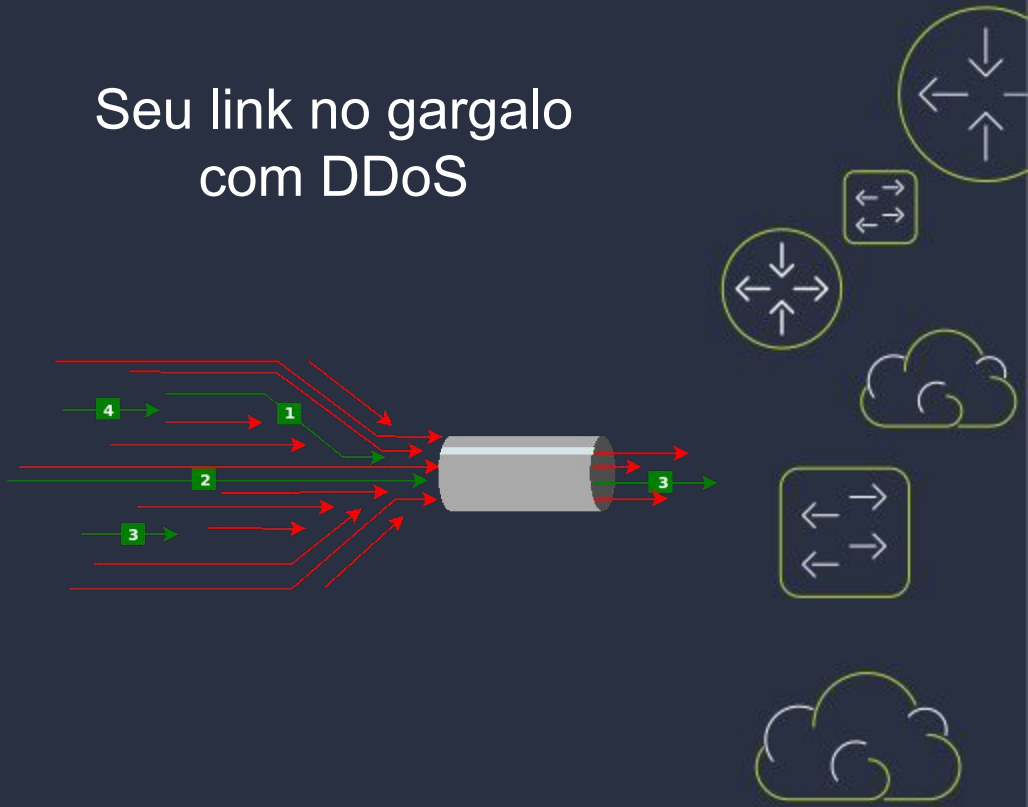
O que é um ataque DDoS

- Inundação de dados maliciosos contra um alvo específico.
- Isto é semelhante a um engarrafamento: as coisas não fluem como deveriam.

O que é um ataque DDoS

Um cano entupido
com sujeira

Seu link no gargalo
com DDoS



Quais são os objetivos do DDoS

- Saturar toda a **banda** disponível com trânsitos IP e IX.
- Saturar a capacidade computacional **(CPU)** de roteadores, concentradores PPPoE e CGNAT.
- Exaurir o **recurso humano** de seu ISP, com jornadas longas de trabalho, filas elevadas no call center.

O que é a mitigação

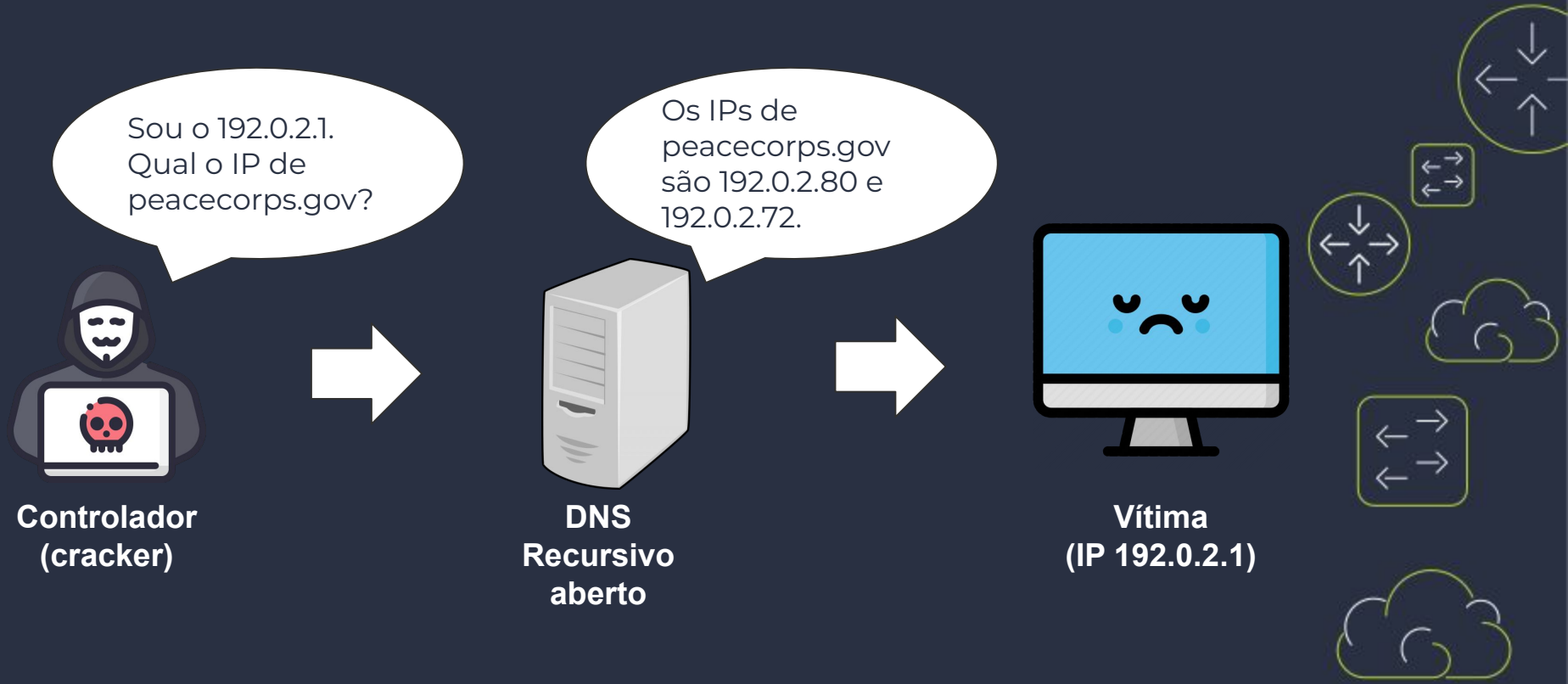
- Um serviço, sistema ou appliance que limpa o tráfego sujo com a finalidade de **reduzir ao máximo os impactos** de um ataque DDoS.

- Ela pode ser feita localmente (*on premise*) ou como um **serviço em nuvem.** Esta segunda forma é mais utilizada na maioria dos casos.

Agora já posso relaxar?

- Após contratarem serviços de mitigação, muitas empresas pensam que nada mais precisa ser feito e apenas relaxam.
- Será que isto é verdade? Vejamos alguns casos.

Ataque de reflexão de DNS



Ataque de reflexão de DNS

- DNSs públicos, inclusive os famosos, participam de ataques DDoS também (em menor escala, mas participam). Veja:

No.	Time	Source	Proto	Length	Info
1405	0.005135	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1430	0.005233	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1466	0.005339	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1498	0.005446	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1522	0.005555	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1559	0.005672	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1580	0.005784	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1610	0.005884	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1639	0.005993	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1660	0.006092	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1680	0.006205	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1710	0.006311	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1735	0.006408	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT
1763	0.006515	8.8.8.8	DNS	91	Standard query response 0x9ec5 Server failure ANY access-board.gov OPT

Ataque de reflexão de DNS

- Quando uma origem faz muitas consultas simultâneas nestes servidores, os DNSs públicos limitam as respostas.

Google Public DNS for ISPs

Anyone, including Internet Service Providers (ISPs) and large organizations, is free to use Google Public DNS, but we apply rate limits to each client to protect our service. High query volumes from a single IPv4 address (or IPv6 /64 network prefix) may be throttled if they exceed these limits.

https://developers.google.com/speed/public-dns/docs/isp

O que fazer então?

- Usar um DNS recursivo local próprio e forçar os clientes a não utilizarem servidores públicos.

- *Se não,* o seu investimento de dezenas de milhares ou milhões foi em vão!

Falando em DNS, amanhã tem:

14:45: 8.888 motivos para não usar DNS recursivo externo em seu AS

Ayub
Sage Networks

15:15: DNS Recursivo Anycast: O que não te contaram por trás do nome bonito

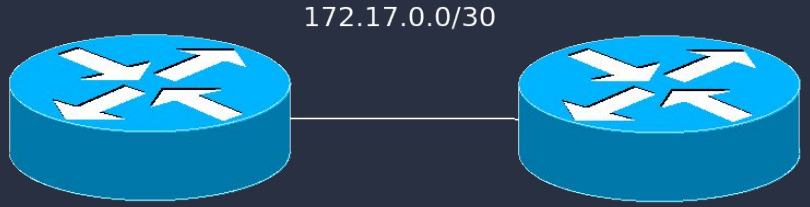
Elizandro Pacheco
Nexthop

Ataques em IP de WAN (backbone)

- Se o IP de P2P (/30 ou equivalente) usado em no enlace entre dois roteadores for atacado, você:
  - Poderá ter dificuldade em fazer RTBH neste IP ou
  - Poderá ter dificuldade para desviar este IP para uma caixa de mitigação ou
  - Terá que desviar todo o /24 para uma nuvem de mitigação.
- Tudo isto para um IP que talvez não precisasse ser público.

O que fazer então?

- Se puder, utilize IPs privados para P2P.
- Se não puder, já tenha o seu roteamento pronto para que um anúncio de RTBH ou desvio de um destes IPs atacados ganhe da rota estática em seu backbone.

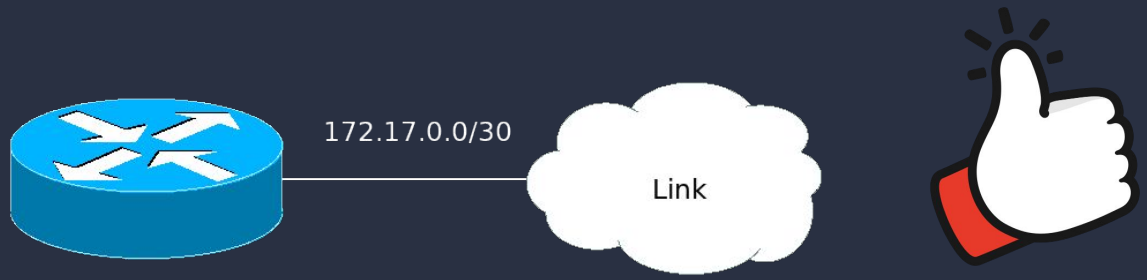


Ataques em IP de WAN (Upstream)

- Se o IP de P2P (/30 ou equivalente) usado em seu roteador para receber o link for atacado, você não pode fazer nada a não ser desligar o link.

O que fazer então?

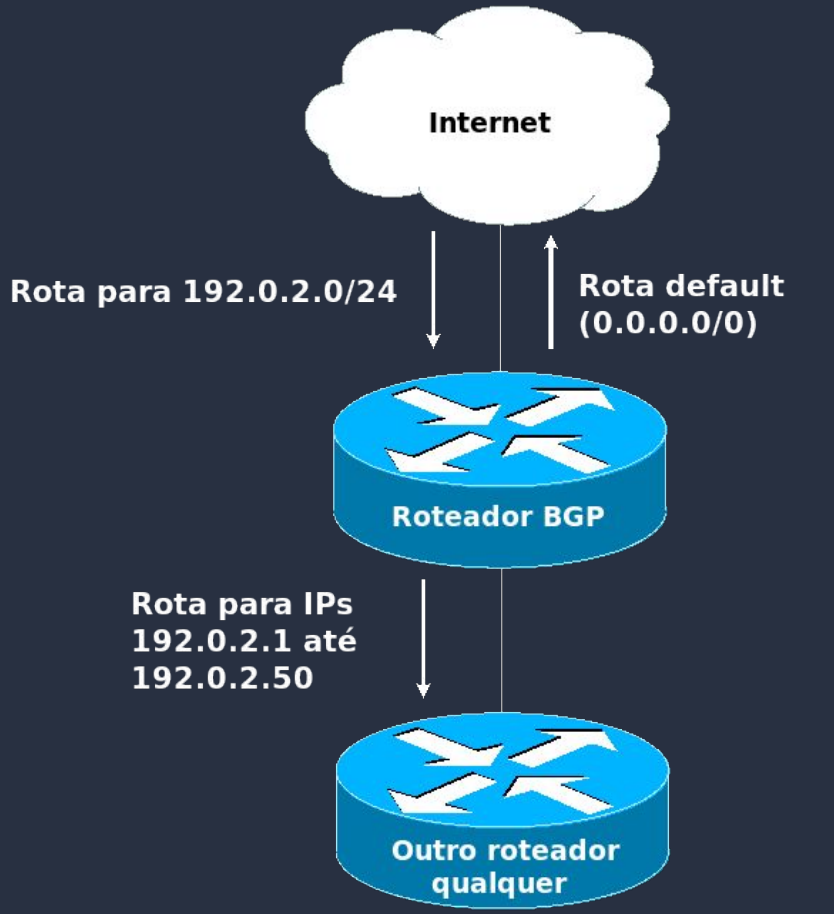
- Peça para seu fornecedor:
  - Fornecer um IP privado ou
  - Deixar o IP público em blackhole ou
  - Proteger (de verdade) este IP.



Loops de roteamento

- Este é provavelmente o problema de rede relacionado à DDoS mais devastador que existe. Ainda que mitiguemos 500 Gbps de um ataque, 300 Mbps que vazar serão suficientes para travar sua rede.

- Veja no próximo slide como isto acontece.


Internet
Rota para 192.0.2.0/24
Rota default
(0.0.0.0/0)
Roteador BGP
Rota para IPs
192.0.2.1 até
192.0.2.50
Outro roteador
qualquer
IPs em uso: 192.0.2.1 até 192.0.2.50

O que fazer então?

1. Aprenda dinamicamente os IPs em uso na tua rede em teu roteador de borda.

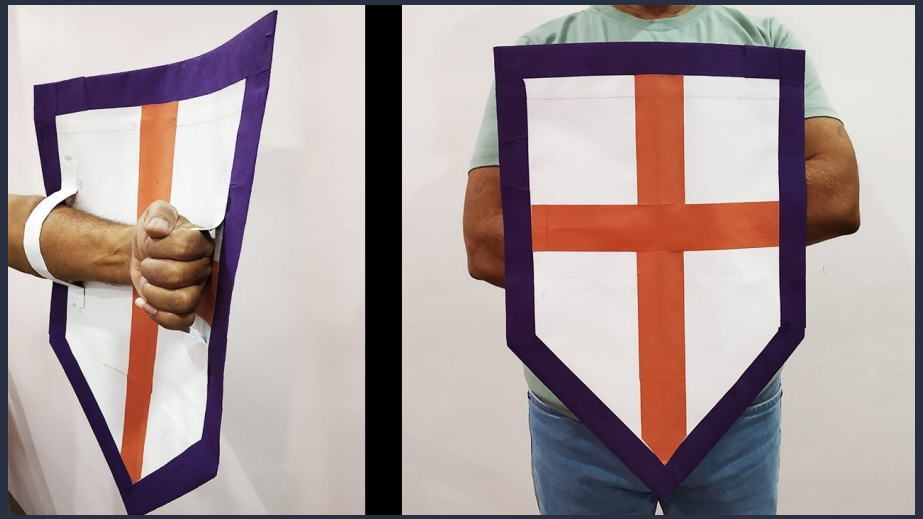
2. Crie uma rota do bloco inteiro (ex: /22) para a blackhole local.

Mitigar ataques com regras de firewall

- Recentemente vi alguém vendendo regras de firewall para mitigar DDoS em Mikrotik.
- Isto não irá funcionar por que:
  - Se o seu link saturar, não adianta descartar o tráfego internamente.
  - O roteador não irá aguentar processar todo o tráfego do ataque.

Mitigar ataques com regras de firewall

- Sua empresa estará protegida assim:



O que fazer então?

1. Contrate um serviço especializado de mitigação;
2. Se possível, troque para um hardware based router. Se não:
    a. Tente usar fastpath e fastrack em sua caixa;
    b. Deixe esta caixa utilizando a menor quantidade de CPU possível.

Resumo das boas práticas

- NÃO use DNS público em sua rede.
- Evite IPs públicos em P2P no teu backbone.
- Evite IPs públicos em P2P com upstreams.
- Fuja dos loops de roteamento.
- Não tente mitigar ataques DDoS com regras de firewall locais.

Outras boas práticas

- Use IPv6. Ele irá te salvar se tudo der errado.
- Não trabalhe próximo aos limites (links, roteadores, enlaces etc).
- Contrate mitigação antes do primeiro ataque.
- Não ouça conselhos técnicos de quem não é especialista.

Isso é tudo, pessoal!

- Dúvidas?

Email: comercial@sagenetworks.com.br
Telefone: 19 3500-6269