Mitigação de DDoS

para ISPs

por T. Ayub
Diretor de Tecnologia

E o que são ataques DDoS?

São ataques a redes dos ISPs e data centers que tem como objetivo deixá-las fora do ar ou com performance severamente degradada.

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

youtube.com/c/ayubio

O que a Sage Networks faz?

Tudo que envolve o anti-DDoS:

- Implantação de sistemas de **detecção** e automação de resposta a ataques.
- **Nuvem** de mitigação por VPN, VLAN bilateral ou cross connect.
- Implantação do produto de mitigação DDoS no **portfólio** de seu ISP ou data center.

Então quem procura a Sage?

- Quem quer montar um centro de mitigação na sua rede para **vender** esse serviço aos seus clientes.
- Quem quer **evitar** que seu negócio fique fora do ar por conta desse tipo de ataque.
- Quem já está totalmente fora do ar **totalmente fora do ar** por conta desses ataques.

- “A cavalaria chegou!”
- “Os bombeiros chegaram!”

… mas na verdade me sinto um outro cara.


É proibido fumar neste local.
Smoking prohibited in this area.

Quais são os 3 modos?

Quais são os 3 modos de se fazer um ISP?

- O modo **errado**.
- O modo **certo**.
-

Quais são os 3 modos?

Quais são os 3 modos de se fazer um ISP?

- O modo **errado**.
- O modo **certo**.
- O modo **resistente** à ataques DDoS.

O que o ISP tem que fazer para fazer um bom uso da mitigação de DDoS?

Sobre o ataque em si

O que você precisa saber:

- O atacante **não** será **identificado**.
- Sua operadora **não** vai **resolver** o problema.
- A temporada de ataque costuma durar **meses**.
- O ataque é fácil e **barato** de ser feito.
- Se você nunca foi atacado, com o passar do tempo o **risco** aumenta.

Bronze Monthly

$ 10 .00

1 Concurrent
300 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Gold Monthly

$ 35 .00

1 Concurrent
1200 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Platinum Monthly

$ 50 .00

1 Concurrent
2500 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Sobre a mitigação

O que você precisa saber:

- A implantação dela dura dias **dias** e não horas.
- Se sua rede não estiver sólida o suficiente você continuará **fora do ar**.
- Ela vai gerar **efeitos colaterais**.

Sobre os efeitos colaterais

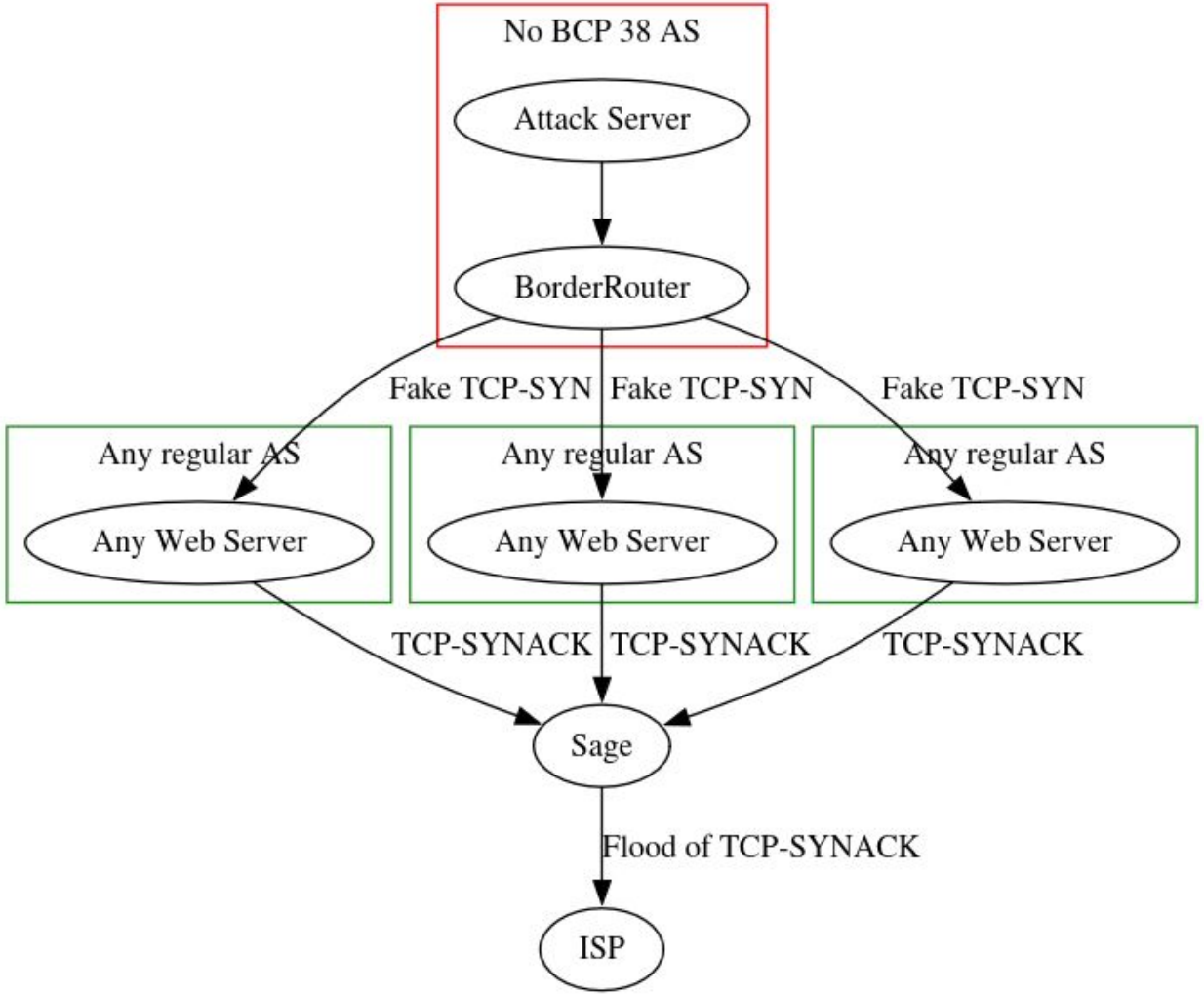
O que você precisa saber:

- Ataques grandes geram **congestionamento** em Tier-1 e até cabos submarinos.
- ITPs, Sistemas Autônomos, nuvens e hospedagens estão colocando IPs brasileiros em **blacklist** por SYN Flood.

Sobre os efeitos colaterais

O que você precisa saber:

- Ataques grandes geram **congestionamento** em Tier-1 e até cabos submarinos.
- ITPs, Sistemas Autônomos, nuvens e hospedagens estão colocando IPs brasileiros em **blacklist** por SYN Flood.


No BCP 38 AS
Attack Server
BorderRouter
Fake TCP-SYN
Fake TCP-SYN
Fake TCP-SYN
Any regular AS
Any regular AS
Any regular AS
Any Web Server
Any Web Server
Any Web Server
TCP-SYNACK
TCP-SYNACK
TCP-SYNACK
Sage
Flood of TCP-SYNACK
ISP

Sobre os efeitos colaterais

O que você precisa saber:

- Ataques grandes geram **congestionamento** em Tier-1 e até cabos submarinos.
- ITPs, Sistemas Autônomos, nuvens e hospedagens estão colocando IPs brasileiros em **blacklist** por SYN Flood.

O que você precisa fazer?

Antes do primeiro ataque:

- Por o **IPv6** em produção. Parcialmente é melhor que nada.
- Rodar seus servidores de DNS **localmente**.
- Trocar seu roteador de borda por um ***hardware based***.

O que você precisa fazer?

- Tenha o controle do seu **roteador de borda**.
- Tenha uma **documentação** impecável de sua rede: IPs em uso, VLANs, topologia, portas.
- Construa um dashboard tático de **gráficos** de sua rede.

O que você precisa fazer?

- Separe seu time de **engenharia** do time do suporte.
- Implante um sistema de **detecção e automação** de resposta a ataques.
- Contrate uma **nuvem de mitigação** antes do primeiro ataque.

Dúvidas?

E-mail: thiago.ayub@sagenetworks.com.br

Site: sagenetworks.com.br