Estudo sobre a anatomia dos ataques de SYN Flood

Daniel Damito

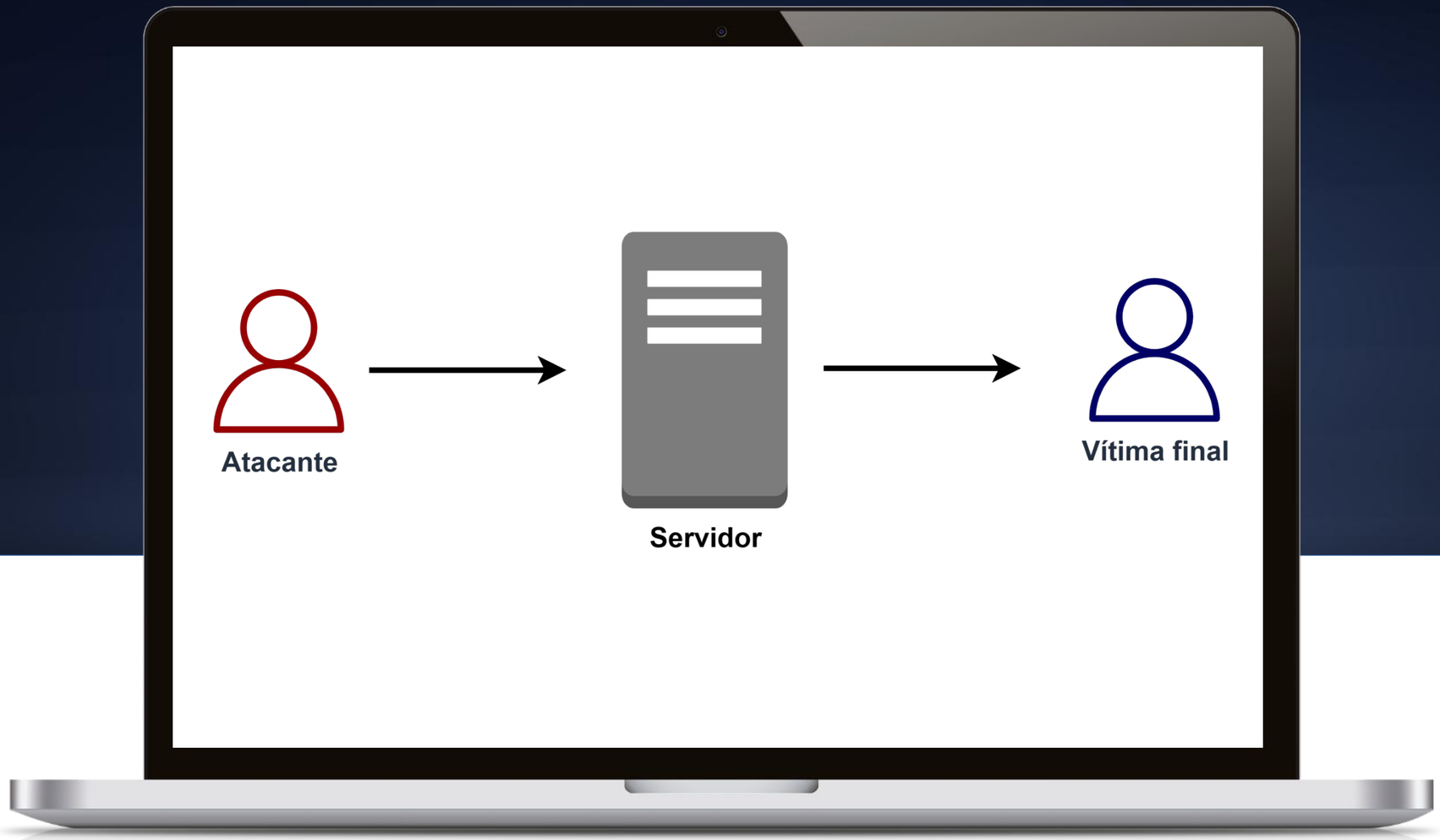
Mayco Berghetti

CONTEXTUALIZAÇÃO

Em 2025, um dos ataques DDoS que mais estiveram em evidência foram os ataques de reflexão de HTTPS, que aqui chamaremos apenas de SYN/ACK.

O objetivo desta apresentação é falar sobre este ataque também do ponto de vista dos servidores, vítimas intermediárias, e não finais.

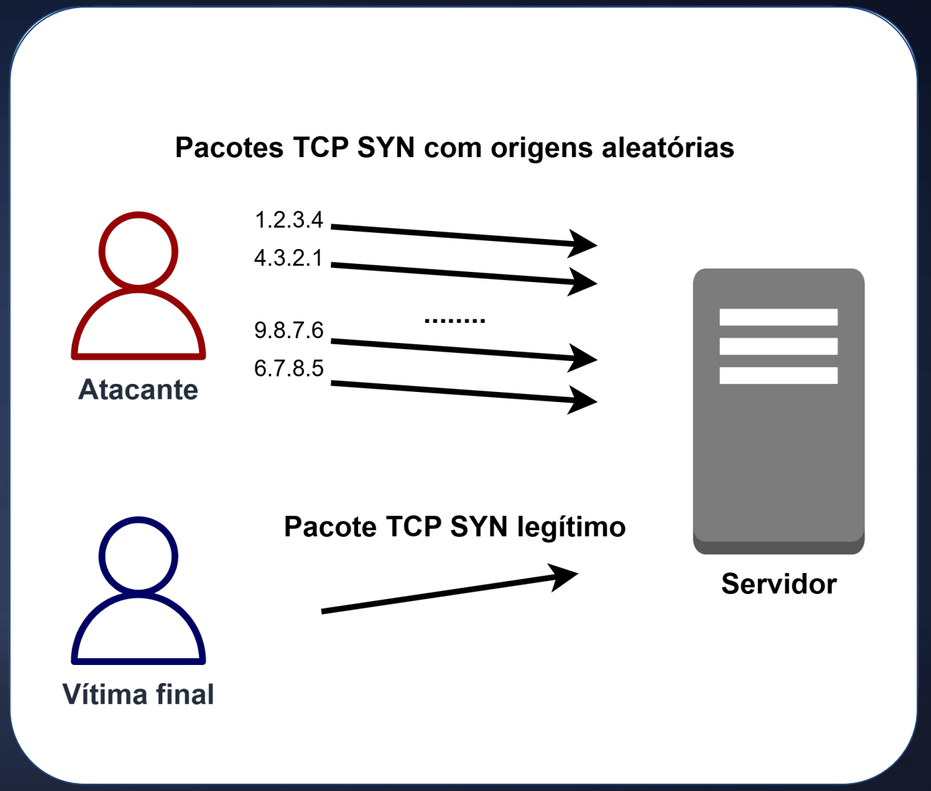
QUEM SÃO OS **PRINCIPAIS ATORES** ENVOLVIDOS NOS ATAQUES DE SYN FLOOD E SYN/ACK FLOOD



HÁ DOIS TIPOS DE OBJETIVO DO SYN FLOOD

1. Para indisponibilizar uma aplicação

- Normalmente os IPs de origem são bastante diversificados.

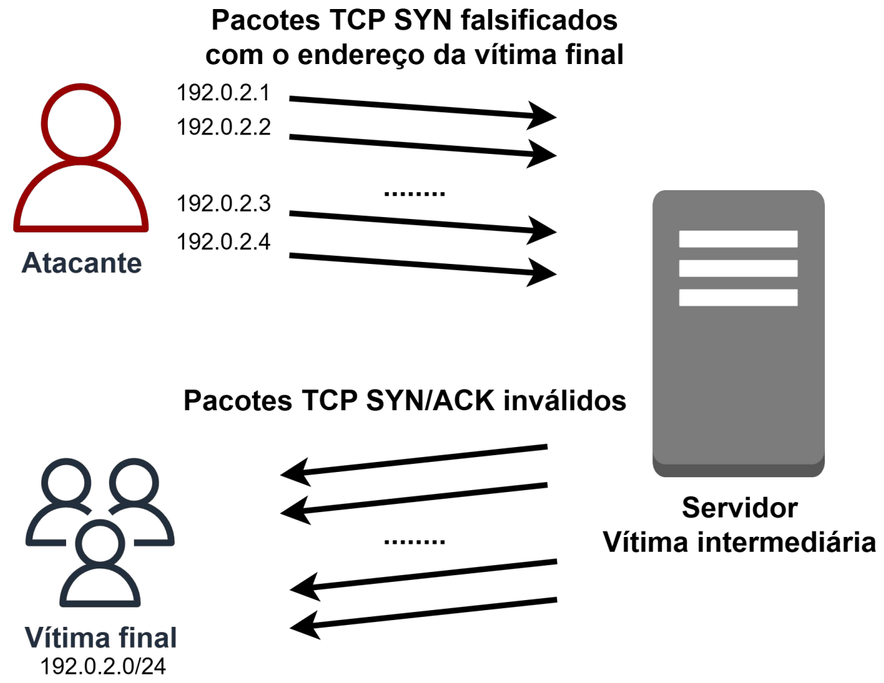


HÁ DOIS TIPOS DE OBJETIVO DO SYN FLOOD

2. Para reflexão

- Normalmente os IPs de origem possuem algo em comum:
  - Pequeno range de IPs
  - ASN
  - Cone de ASN

- O servidor também pode enviar Challenge ACK (RCF 5961), gerando também ACK flood.



SYN FLOOD: PROBLEMAS CAUSADOS

- Equipamentos saturados (servidores, roteadores)
- Links saturados
- Falhas no acesso a conteúdos específicos
  - Alguns servidores limitam eventualmente o tráfego dos IPs das vítimas que foram forjados.

AMPLIFICAÇÃO DOS ATAQUES DE SYN/ACK FLOOD

Na configuração padrão, Linux envia **5** retransmissões de SYN/ACK em 31 segundos.

	Time	Source	Destination	Protocol	Length	Info
3	0.017747889	10.0.0.2	10.0.0.1	TCP	60	12345 → 443 [SYN] Seq=0 Win=8192 Len=0
4	0.017901007	10.0.0.1	10.0.0.2	TCP	60	443 → 12345 [SYN, ACK] Seq=0 Ack=1 Win=6424
5	1.040423823	10.0.0.1	10.0.0.2	TCP	60	[TCP Retransmission] 443 → 12345 [SYN, ACK]
6	3.088527944	10.0.0.1	10.0.0.2	TCP	60	[TCP Retransmission] 443 → 12345 [SYN, ACK]
9	7.120478847	10.0.0.1	10.0.0.2	TCP	60	[TCP Retransmission] 443 → 12345 [SYN, ACK]
10	15.504124337	10.0.0.1	10.0.0.2	TCP	60	[TCP Retransmission] 443 → 12345 [SYN, ACK]
11	31.888544411	10.0.0.1	10.0.0.2	TCP	60	[TCP Retransmission] 443 → 12345 [SYN, ACK]

AMPLIFICAÇÃO DOS ATAQUES DE SYN/ACK FLOOD

Em uma amostragem durante um ataque de SYN/ACK, mais de **50%** dos pacotes eram **retransmissões** de pacotes SYN/ACK

```
$
$ tshark -r attack.pcap | wc -l
3210016
$ tshark -r attack.pcap -Y "tcp.analysis.retransmission and tcp.flags.syn == 1 and tcp.flags.ack == 1" | wc -l

1705361
$ echo $((1705361*100/3210016))%
53%
$
```

COMO MITIGAR O SYN FLOOD (PONTO DE VISTA DO SERVIDOR)

- Se você é conteúdo, rate limit **não** é a melhor opção.
  - Pode limitar tráfego legítimo indevidamente;

COMO MITIGAR O SYN FLOOD (PONTO DE VISTA DO SERVIDOR)

- Habilitar SYN cookies no servidor (Linux: *tcp_syncookies*).
  - Evita alocação de recursos até que a conexão seja estabelecida
- Limitar retransmissão de pacotes SYN/ACK no servidor (Linux: *tcp_synack_retries*).
  - Reduz o envio de retransmissões e a carga de rede
- Utilizar um servidor SYNPROXY.
  - Servidor dedicado para validar conexões
- Mais na RFC 4987 (TCP SYN Flooding Attacks and Common Mitigations).

Ao limitar as retransmissões reduzimos a amplificação de um ataque SYN/ACK.

```
> cat /proc/sys/net/ipv4/tcp_synack_retries
0
```

	Time	Source	Destination	Protocol	Length	Info
3	0.019169051	10.0.0.2	10.0.0.1	TCP	60	12345 → 443 [SYN] Seq=0
4	0.019257497	10.0.0.1	10.0.0.2	TCP	60	443 → 12345 [SYN, ACK]

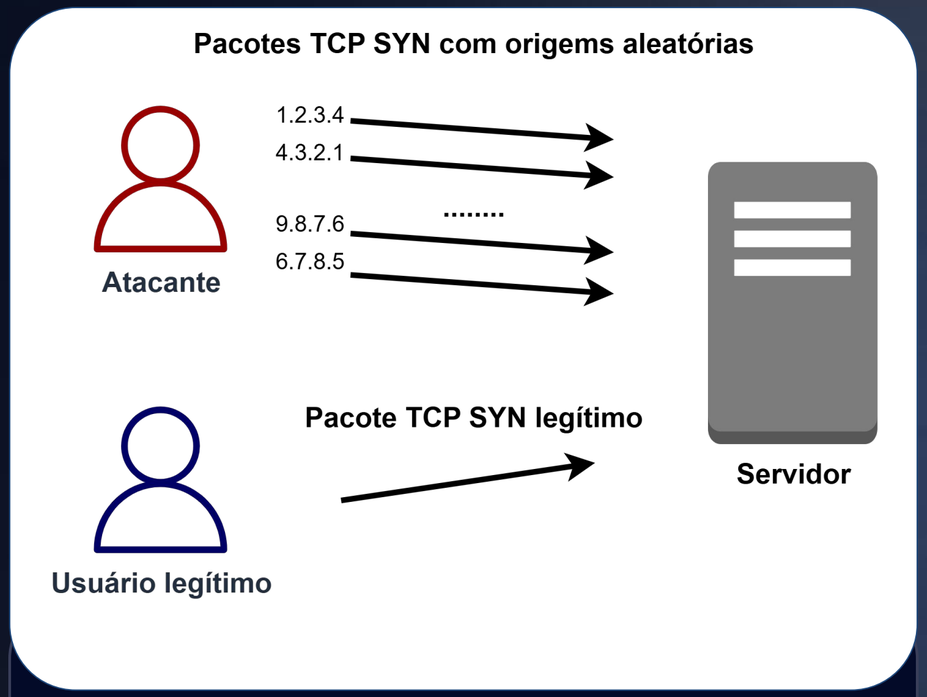
COMO MITIGAR O SYN/ACK FLOOD (PONTO DE VISTA DA VÍTIMA FINAL)

- Monitorar o TCP handshake e descartar pacotes inválidos (SYN/ACKs sem SYNs correspondentes). Aqui é necessária uma mitigação statefull.

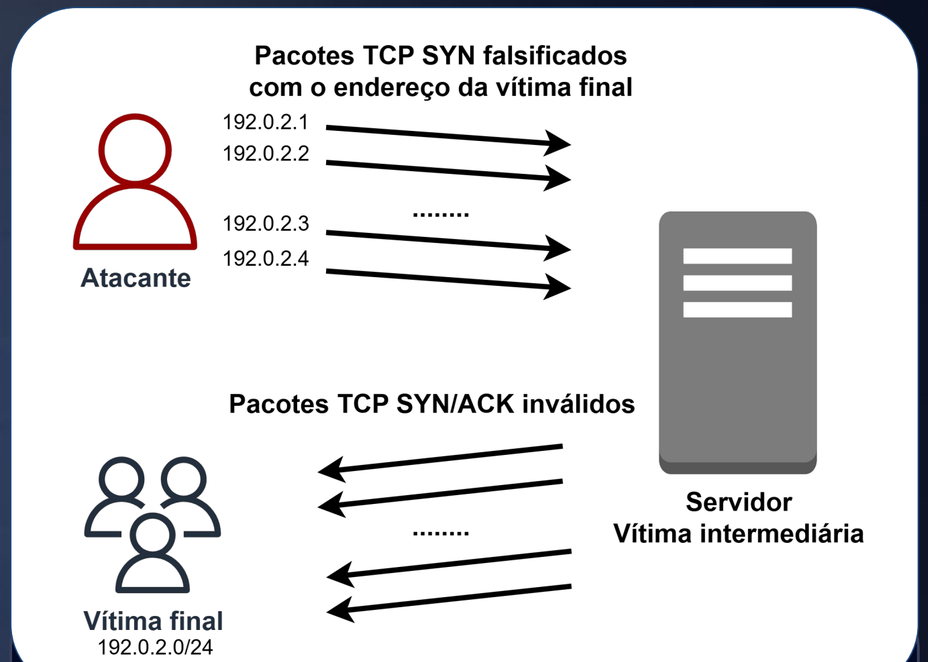
- Utilizar uma solução especializada que identifica tráfego malicioso.
  - Projetadas para o caso de DDoS (diferente de firewalls convencionais)
  - Utiliza diferentes estratégias e algoritmos

- No geral, rate limit de SYN/ACK amplifica o dano do DDoS. (não fazer)

RESUMO



- Você recebendo o SYN Flood
- Mitigação:
  - Utilizar SYN cookies.
  - Reduzir retransmissões de SYN/ACK.
  - Utilizar SYNPROXY.



- Você recebendo o SYN/ACK Flood
- Mitigação:
  - Monitorar TCP handshake e descartar pacotes inválidos.
  - Algoritmo avançado de testagem.
    - Solução industrial

SAGE NETWORKS

WWW.SAGENETWORKS.COM.BR

sage_networks Sage Networks +55 (19) 3500-6269