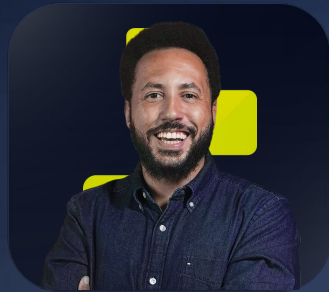


Anti-DDoS para Sistemas Autônomos



Daniel Damito



Thiago Ayub

DIA 3 - ESTRATÉGIAS DE MITIGAÇÃO E OPERAÇÃO - DAMITO



- Você nunca será capaz de mitigar um ataque DDoS com maestria se não:
 - a) entender redes.
 - b) não souber capturar pacotes.
 - c) não souber interpretar uma captura.

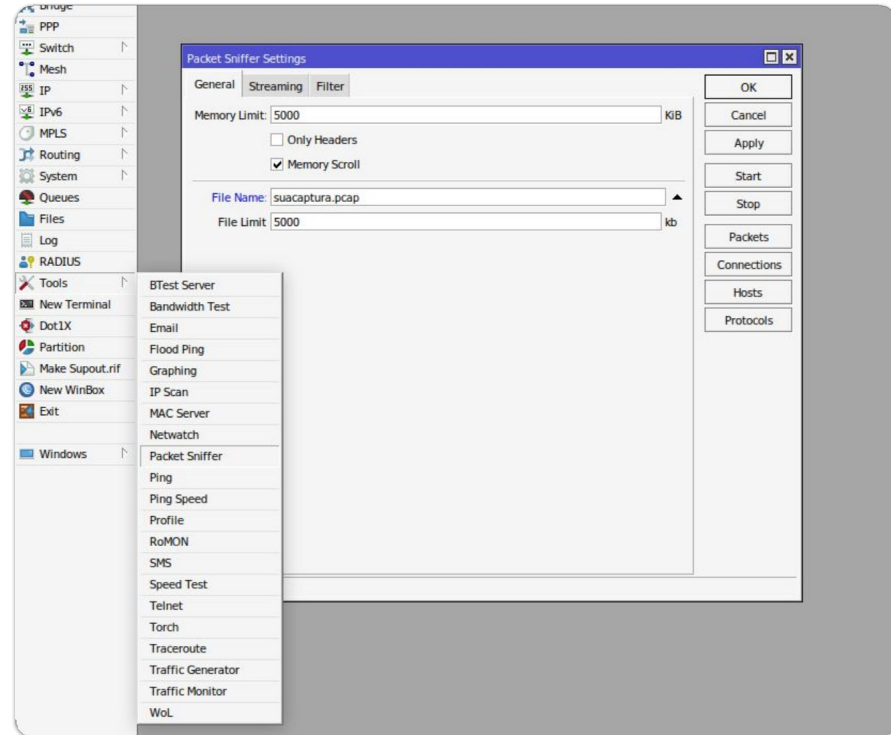
- Recomendo assistir este conteúdo sobre o assunto para se aprofundar:
<https://www.youtube.com/watch?v=oQVO51j9StE&t=2s>



CAPTURANDO PACOTES PARA ANÁLISE



- **Mikrotik (meu método preferido):**
 - A opção mais fácil!
 - Você pode ver em tempo real ou salvar captura em seu computador.
 - [https://wiki.brasilpeeringforum.org/w/Como capturar pacotes no Mikrotik](https://wiki.brasilpeeringforum.org/w/Como_capturar_pacotes_no_Mikrotik)



CAPTURANDO PACOTES PARA ANÁLISE



- **Huawei, Cisco, Nokia e Juniper:**

- Fácil de capturar pela praticidade de o tráfego já estar passando pelos roteadores.
- <https://sagenetworks.com.br/embedded-packet-capture-cisco/>
- <https://sagenetworks.com.br/captura-de-pacotes-no-junos-os/>
- <https://sagenetworks.com.br/captura-de-pacotes-em-roteadores-huawei-vrp/>

CAPTURANDO PACOTES PARA ANÁLISE



- **Linux (TCP Dump):**
 - Exige direcionar o tráfego para uma máquina, mas vale o esforço.

O QUE VOCÊ DEVE BUSCAR EM SUAS CAPTURAS



- Pacotes que violem regras claras de RFCs ou protocolos.
 - Ex: 1) TCP com todas as flags ou 2) SSDP (UDP/1900) fora de LAN.
- Comportamentos que levantam suspeita.
 - Ex: Excesso de pacotes TCP com porta de origem e destino baixas, ao mesmo tempo.
- Excesso de padrões repetidos.
 - Ex: 1) Maioria dos pacotes com um mesmo tamanho ou 2) Excesso de pacotes com flag atípica, como PSH ou RST.
- Tráfego acima do normal para um dado protocolo.
 - Ex: Maioria dos pacotes sendo respostas DNS.

EXERCÍCIO: MITIGUE O ATAQUE



No.	Time	Source IP	Destination IP	Proto	Len	Info
[]	0	0 192.168.1.45	192.0.2.14	TCP	74	54321 → 8080 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	1	1.245 45.33.2.112	192.0.2.87	TCP	74	12345 → 9000 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	2	2.132 185.199.108.153	192.0.2.203	TCP	74	60500 → 4444 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	3	3.567 104.26.10.19	192.0.2.56	TCP	74	33890 → 2022 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	4	4.891 93.184.216.34	192.0.2.87	TCP	74	55678 → 3000 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	5	5.122 23.45.162.12	192.0.2.142	TCP	74	49152 → 5050 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	6	6.789 151.101.1.69	192.0.2.9	TCP	74	62001 → 1001 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	7	7.432 13.224.161.44	192.0.2.221	TCP	74	80 → 8888 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	8	8.901 31.13.71.36	192.0.2.56	TCP	74	51234 → 6500 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	9	9.543 52.84.162.240	192.0.2.178	TCP	74	22022 → 4433 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	10	10.121 18.160.124.55	192.0.2.34	TCP	74	58901 → 27017 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	11	11.654 104.18.2.161	192.0.2.199	TCP	66	443 → 51234 [ACK] Seq=1 Ack=1 Win=65536 Len=0
[]	12	12.342 8.8.8.8	192.0.2.87	UDP	82	53 → 54321 DNS Standard query response
[]	13	13.876 172.67.13.15	192.0.2.61	TCP	74	443 → 62102 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	14	14.543 66.220.144.11	192.0.2.145	TCP	74	40123 → 5060 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	15	15.921 157.240.222.35	192.0.2.3	TCP	74	33000 → 6379 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	16	16.345 104.244.42.1	192.0.2.250	TCP	74	55443 → 8000 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	17	17.892 199.16.156.198	192.0.2.112	TCP	74	10250 → 1234 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460
[]	18	18.543 204.79.197.200	192.0.2.56	TCP	74	61111 → 2000 [SYN, ACK] Seq=0 Ack=1 Win=64240 MSS=1460

EXERCÍCIO: MITIGUE O ATAQUE



- Considere que:
 - A rede de destino é a 192.0.2.0/24.
 - Esta é uma rede predominantemente eyeball, que **consume** conteúdo. Não há provimento de conteúdo através dela de forma relevante.
 - Não existe upload de sua rede nesta captura, apenas download.

EXERCÍCIO: MITIGUE O ATAQUE



- O caos está instaurado:
 - A fila de chamados está crescendo.
 - A rede está parada.
 - O maior cliente já sinalizou que está prestes a cancelar.
- Escreva A (accept) na esquerda de todo pacote que você entenda que deve ser aceito na mitigação.
- Escreva D (discard) na esquerda de todo pacote que você entenda que deve ser aceito na mitigação.

EXERCÍCIO: MITIGUE O ATAQUE



- **Gabarito:**
 - **Pacotes legítimos:** 7, 11, 12, 20, 27, 30, 42, 49.

EXERCÍCIO: MITIGUE O ATAQUE



Reflexão:

- Quem dropou um pacote legítimo, qual efeito colateral causou ao fazer isto?
- Você crê que este discard valeu a pena, considerando o contexto maior do ataque e da indisponibilidade?
- A mitigação quase sempre será imperfeita. É melhor descartar pacotes demais e ter mais colaterais, ou vaziar mais ataques, tendo menos colaterais?

MITIGANDO UM ATAQUE LOCALMENTE



Requisitos:

1. Capacidade de interconexão com a Internet.
 - a. Uso estratégico do IX.
2. Capacidades de roteadores.
3. Equipamento de mitigação local.
4. Possibilidade de chaveamento fácil para a mitigação (ferramenta de desvio e detecção).

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

- Ataques DDoS podem chegar por todos os caminhos:
 - Trânsitos.
 - IX's.
 - PNI's.
 - Caches.
 - Downstreams.
 - Outros tipos de peers.

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

- Para ter a capacidade de mitigar X Gbps de ataque, você precisa ter a capacidade **total** de X Gbps + o pico do teu consumo real.
 - Exemplo:
 - Teu pico de consumo é de 100 Gbps.
 - Você quer mitigar até 300 Gbps.
 - Tua capacidade total precisa ser de 400 Gbps.
- Mas do que é composta a “capacidade total”?

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

Capacidade total:

- O único lugar que você pode **garantir** plenamente a capacidade é no trânsito IP/Upstream, pois ele tem a premissa de alcançabilidade total na Internet.
- Mas considerando que os ataques costumam chegar por vários lugares ao mesmo tempo, você também pode contabilizar seus outros caminhos.

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

Cenário de exemplo:

- Capacidade com upstreams: até 200 Gbps (contando com burst).
- Capacidade com IX: até 300 Gbps.
- PNI's: até 100 Gbps.

Neste exemplo, até quanto podemos mitigar de ataques DDoS no melhor cenário?

- 600 Gbps.

E no pior cenário?

- 200 Gbps.

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

Esta matemática não é muito exata, então evite complicações ao divulgar a capacidade do Anti-DDoS.

Exemplo anterior de uma forma menos complicada:

- Capacidade de mitigação: de 200 à 600 Gbps total.

MITIGANDO UM ATAQUE LOCALMENTE



1. Capacidade de interconexão com a Internet

- Como o IX me ajuda nisso?
 - Tráfego mais barato;
 - Possibilidade de fazer anúncios seletivos;
 - Possibilidade de RTBH (blackhole);
 - Possibilidade de identificar o MAC de origem.



MITIGANDO UM ATAQUE LOCALMENTE



2. Capacidade de roteadores

- Softrouters e DDoS são inimigos mortais.
 - Softrouters utilizam CPU para todo encaminhamento de pacotes.
 - A CPU se torna gargalo.
- Para mitigar ataques DDoS com menos sofrimento, vá de hardware based router, como Cisco, Huawei, Nokia e Juniper.
- Estes HBR encaminham pacotes sem o uso da CPU.

MITIGANDO UM ATAQUE LOCALMENTE



2. Capacidade de roteadores

- Procure por roteadores que suportem a maior quantidade possível de:
 - ACLs.
 - Regras de FlowSpec.
 - Encaminhamento de pacotes por segundo.
 - Densidade de portas.
 - Portas com a maior largura de banda possível.
 - Suporte à FlowSpec Redirect, por VRF e Nexthop.
- Desejável:
 - Teste o FlowSpec Redirect antes da compra.
 - Possua suporte do fabricante.

MITIGANDO UM ATAQUE LOCALMENTE



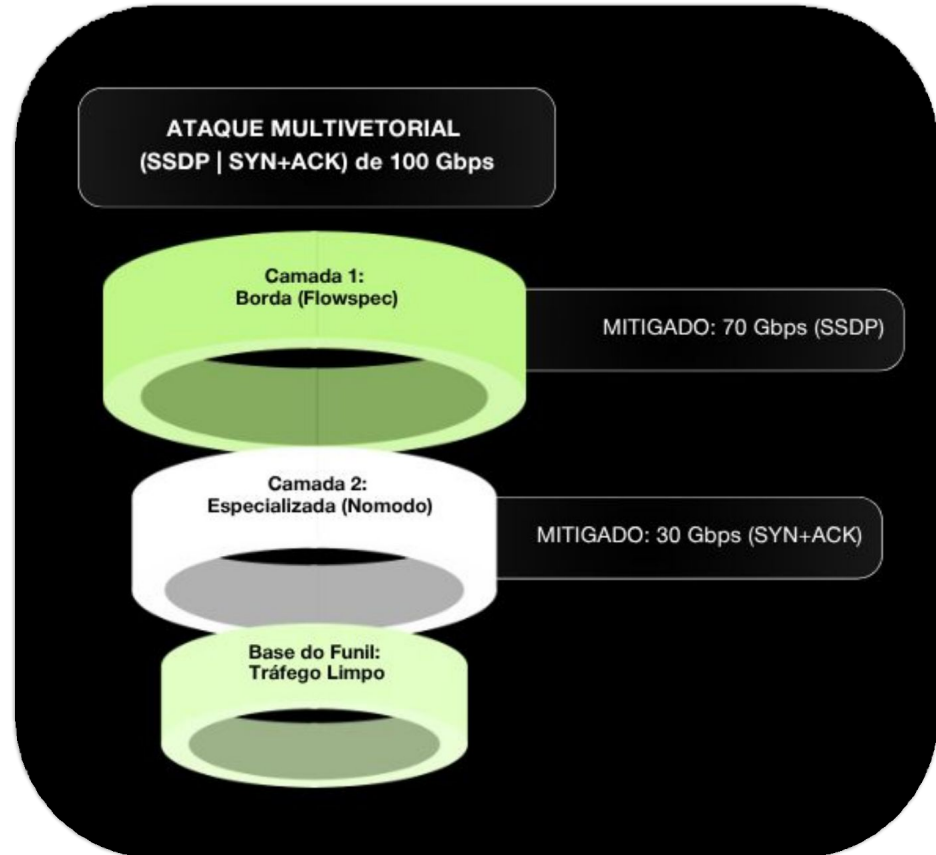
3. Equipamento de mitigação local

- Você pode trabalhar apenas com FlowSpec, mas isso te trará uma mitigação mais limitada.
- Recomendo o curso que fizemos com o NIC.br em flowspec.com.br. É online e gratuito!
- Para otimizar, adote o modelo híbrido de mitigação local com FlowSpec + caixa de mitigação (funil de mitigação, imagem no próximo slide).

MITIGANDO UM ATAQUE LOCALMENTE



3. Equipamento de mitigação local



MITIGANDO UM ATAQUE LOCALMENTE



3. Equipamento de mitigação local

- Para se mitigar plenamente, escolha um equipamento de mitigação local especializado. Mas tenha ciência de que uma única caixa não resolverá todos os seus problemas.
- Cada equipamento possui seus pontos fortes e fracos.
- Tenha mais de um vendor de mitigação on-premise ou busque por um equipamento com bastante flexibilidade.

MITIGANDO UM ATAQUE LOCALMENTE



3. Equipamento de mitigação local

- Requisitos a se buscar em uma caixa de mitigação:
 - A possibilidade de criar regras de mitigação personalizadas. Quanto mais possibilidades de matchers, melhor.
 - Sistemas que lancem atualizações ou novas vacinas frequentemente.
 - Algoritmos inteligentes para testes de licitude em conexões TCP.
 - Interface gráfica para acompanhamento do tráfego total, mitigado e pós mitigado.
 - Suportar uma elevada quantidade de pps.
 - Suporte nos moldes exigidos pela sua operação (horário de atendimento, SLA e idioma).
 - Outros requisitos técnicos precisam ser avaliados a depender da operação.

MITIGANDO UM ATAQUE LOCALMENTE



3. Equipamento de mitigação local

- Adicional:
 - Editais públicos costumam exigir mitigação on-premises. Busque por caixas que atendam os principais critérios exigidos nestes editais.

MITIGANDO UM ATAQUE LOCALMENTE



4. Possibilidade de chaveamento fácil para a mitigação

- Você deve possuir uma ferramenta de desvio automático que seja capaz de:
 - Detectar ataques de forma abrangente:
 - Carpet bombing.
 - Hit & Run.
 - pps e bps.
 - Contra subredes ou IPs individuais.
 - Preferencialmente suportar Netflow, sflow e port mirroring.
 - Gerar amostras de ataques.
 - Gerar relatórios sobre ataques.
 - Permitir a criação de novos padrões de ataques a serem identificados.

MITIGANDO UM ATAQUE LOCALMENTE



4. Possibilidade de chaveamento fácil para a mitigação

- Ao identificar um ataque, a ferramenta precisa ser capaz de:
 - Desviar blocos por Unicast (máscara customizável, ex: /24, /23, /32).
 - Desviar blocos por FlowSpec Redirect (Next-hop e VRF) seletivamente por protocolo, porta ou outros critérios.
 - Corrigir AS-PATH em anúncios Unicast.
 - Aplicar regras de BGP FlowSpec específicas, não apenas de discard geral (Ex: UDP src port 53 & dst port <1000).
 - Tomar ações diferentes para redes diferentes, se necessário.
 - Especificar, no anúncio gerado, as communities BGP necessárias e o next-hop a serem enviados para o roteador.

MITIGANDO UM ATAQUE REMOTAMENTE



- Mitigação em nuvem, clean pipe e scrubbing remoto costumam ser sinônimos.
- Vantagens:
 - Não existe a necessidade de se investir em CAPEX.
 - Possibilidade de trocar de fornecedor mais facilmente.
 - Escalabilidade em tamanho dos ataques.
- Desvantagens:
 - Aumento da latência em algum nível.
 - Não é possível garantir como a mitigação será feita (algoritmos avançados ou rate-limits simples, por ex).
 - Pouca possibilidade de customização.
 - Geralmente não atende aos critérios de licitações públicas.
- Ainda exige um sistema de detecção automática localmente!

MITIGANDO UM ATAQUE REMOTAMENTE



- Parâmetros a se analisar:
 - 1) Forma de conexão: GRE, VLAN Bilateral ou Cross Connect.
 - 2) Commit e burst de banda limpa.
 - 3) ASNs ou prefixos protegidos.
 - 4) Tipos de ataques suportados.
 - 5) Limite de ataques.
 - 6) Ações necessárias para início da mitigação.

MITIGANDO UM ATAQUE REMOTAMENTE



1. Forma de conexão:

- GRE:
 - Usar clamp-mss.
 - Utilizar IPv6 ou um IP de outro sistema autônomo, que não apareça em traceroutes/mtrs.
 - Ter mais de um, sempre, por redundância.

- VLAN Bilateral:
 - A banda é compartilhada com o tráfego do IX.
 - Mantenha um GRE de redundância se possível.

- Cross Connect:
 - A melhor opção.
 - Circuito garantido.
 - Possui um custo mensal com o datacenter.
 - Mantenha um GRE de redundância se possível.

MITIGANDO UM ATAQUE REMOTAMENTE



2. Commit e burst de banda limpa

- Geralmente a mitigação em nuvem é cobrada pela quantidade de banda limpa (commit e burst), mas existem casos que cobram por franquia de dados, como redes móveis de celular.
- Quanto comprar?
 - Obrigatoriamente um burst que cubra o total de tráfego que tua rede tem de download.
- Entenda o 95th percentile para ter economia.

MITIGANDO UM ATAQUE REMOTAMENTE



3. ASNs e prefixos protegidos

- O fornecedor de mitigação provavelmente irá cobrar valores variáveis de acordo com a quantidade de ASNs ou prefixos a serem protegidos. Isso é comum e esperado. Você deve escolher um plano que cubra todos os ASNs e prefixos que deseja proteger.

4. Tipos de ataques suportados

- Além dos ataques mais comuns, a mitigação precisa ser capaz de proteger ao menos:
 - Ataques de camada 4 e camada 7.
 - Ataques de carpet bombing.
 - Ataques de reflexão TCP (como HTTPS Reflection/SYN ACK).

MITIGANDO UM ATAQUE REMOTAMENTE



5. Limites de ataques

- Analisar se há e quais são os limites da mitigação:
 - Tempo total de ataques no mês.
 - Quantidade de ataques simultâneos ou blocos protegidos ao mesmo tempo.
 - Tamanhos máximos (em pps ou bps) de ataques suportados.

6. Ações necessárias para início da mitigação:

- Geralmente basta anunciar o bloco para o fornecedor, mas eventualmente coisas manuais podem ser pedidas:
 - Ligação ou abertura de chamado sempre que um ataque iniciar.
 - Inserção de community BGP específica.
 - Apertar algum botão para início da mitigação.
- Quanto mais automática a mitigação, melhor. Busque por mitigações que você só precise contatar quando tiver algum problema.

MITIGANDO UM ATAQUE REMOTAMENTE



Mitigação inclusa no trânsito IP

- Por não ser um serviço final das operadoras de trânsito IP, é comum historicamente que elas vendam serviços muito básicos ou limitados apenas pela questão do SVA;
- O que analisar:
 - Se a proteção está incluída no contrato de fato (e não apenas uma promessa de boca).
 - Quais os limites de ataque suportados.
 - Se existe um time especializado em Anti-DDoS neste fornecedor.
- Se possível, tenha uma mitigação especializada também, além de um eventual trânsito IP protegido.

MITIGANDO HÍBRIDA



Um bom custo benefício é se ter uma mitigação local + mitigação em nuvem.

- Como funciona:
 - Você possui uma infraestrutura de mitigação local (caixa de mitigação, tráfegos IPs ociosos, roteadores com FlowSpec etc) que tenham limites mais baixos do que em um cenário de mitigação totalmente local. Ex.: 100 Gbps de tráfegos ociosos + caixa de mitigação local de 100 Gbps.
 - Quanto algum destes limites é atingido, todo o ataque é desviado para um scrubbing center remoto.
- Este é o modelo mais usado em médias empresas.

MITIGANDO HÍBRIDA



- **Quais limites se observar:**
 - Interconexões (Trânsitos IPs, IX's, PNIs etc).
 - Capacidade dos equipamentos de mitigação local.
 - Quantidade de pps suportado pelos roteadores locais.
 - Quantidade de regras de FlowSpec suportadas pelos roteadores locais.

MITIGANDO HÍBRIDA



- Pontos positivos:
 - Traz certo nível de autonomia.
 - Baixa latência para ataques suportados localmente.
 - Menos alterações de propagação no BGP.
 - Atende aos critérios de muitas licitações.
- Pontos negativos:
 - Exige maior confiabilidade do sistema de detecção para automatizar o desvio quando o limite local é atingido.
 - Exige mais perícia do time de redes para fornecer os parâmetros de monitoramento dos limites locais.

POR QUE EXISTEM EFEITOS COLATERAIS E/OU VAZAMENTOS?



Em um cenário utópico, seríamos capazes de inspecionar 100% do tráfego em 100% do tempo em um equipamento de mitigação on-premises avançado. Além disso, deveríamos também ser capazes de analisar o upload para ter uma mitigação statefull.

Mas isto não é possível por uma questão de custos, principalmente. O custo da Internet cai vertiginosamente ao longo dos anos, enquanto a quantidade do tráfego entregue sempre cresce.

2015

10 Mbps: R\$100

2026

600 Mbps: R\$94,90

POR QUE EXISTEM EFEITOS COLATERAIS E/OU VAZAMENTOS?



O cenário utópico descrito é muito diferente do cenário real, que é imperfeito. O cenário real costuma ter mitigações mais sob demanda, seletivas e dinâmicas, sem sequer observar o upload.

Alguns exemplos de onde estes modelos reais falham:

- Quando uma determinada origem de tráfego não segue à risca um comportamento descrito na RFC, como, por exemplo, o tempo de retransmissão de um pacote TC.
- Quando um ataque copia de forma perfeita o comportamento de um tráfego legítimo.
- Quando uma rede não segue boas práticas, por exemplo:
 - Usando um DNS público (que participa de ataques) em vez de um DNS Local.
 - Não utiliza IPv6.
 - Tem loops de roteamento internos.

TROUBLESHOOTING DE VAZAMENTOS



- Vazamentos não devem ser considerados sempre problemas.
- PARE DE OLHAR APENAS PARA O GRÁFICO!
- Eles só devem ser considerados problemas se saturarem algo em sua rede, como:
 - CPU de algum roteador.
 - CPU de algum servidor.
 - Tabela de conexões do CGNAT (Conntrack).
 - Saturação de alguma interface interna ou externa.
 - Saturação de algum outro recurso computacional, como capacidade de pps de um roteador.

TROUBLESHOOTING DE VAZAMENTOS



1. Identifique o problema causado pelo vazamento.
2. Decida o caminho mais rápido: **a)** expandir a capacidade do objeto do gargalo ou **b)** bloquear o tráfego excedente de forma rápida.
 - Isto pode ser feito com fine tuning em roteador, servidor ou CGNAT ou expandindo uma interface de 10 Gbps para 40 Gbps, por exemplo.
 - Você deverá analisar, através de capturas de pacote ou amostras de tráfego, o que está vazando. Identificado o vazamento, o bloqueio deve ser feito no lugar mais fácil e rápido que você puder, como ACL ou FlowSpec local. Um bom sistema de detecção permite regras de FlowSpec customizadas rapidamente.

New Flowspec Rule

BGP Connector: Static_Flowspec

Flowspec Rule

IP Protocol(s):	TCP	Source Port(s):	>1000
Source Prefix:	Any	Destination Port(s):	<1000
Destination Prefix:	192.0.2.0/24	IP Fragment:	Any
Packet Length(s):	Any	DSCP:	Any
TCP Flag(s):	FIN	ICMP Code(s):	Any
ICMP Type(s):	Any		
Action:	Discard		

TROUBLESHOOTING DE VAZAMENTOS



3. Apagado o incêndio, resolva o problema de forma definitiva. Automatize novas regras de FlowSpec para este tipo de ataques, crie novas regras de mitigação em sua caixa de mitigação ou converse com seu fornecedor de mitigação remota.

TROUBLESHOOTING DE EFEITOS COLATERAIS



- Identifique a queixa do problema da forma mais específica possível.
 - O site está lento de fato ou alguns componentes da página web não abrem nunca?
 - O sistema que não abre exibe qual erro?
 - O problema acontece em dispositivos móveis ou pelo computador?
 - O sintoma foi verificado em qual SO?
 - Qual erro aparece?

TROUBLESHOOTING DE EFEITOS COLATERAIS



- **NÃO SEJA GENÉRICO AO REPORTAR O PROBLEMA AO SEU FORNECEDOR!**
 - Exemplo ruim: “Não abre nenhum site”
 - Exemplo bom: “A rede 192.0.2.0/24 não consegue abrir quase nenhum site, apesar de UDP e DNS funcionarem normalmente. Também noto que o tráfego está abaixo do normal para o período (...)”
 - Exemplo ruim: “O site da prefeitura não abre.”
 - Exemplo bom: “Vejo que os pacotes TCP SYN/ACK do site www.xpto.com.br, IP 192.0.2.1 não estão chegando para mim. Outros sites estão abrindo normalmente (...)”.

TROUBLESHOOTING DE EFEITOS COLATERAIS



Exemplo 1 de troubleshooting:

1. Tente capturar pacotes em um ambiente que o problema **não ocorra**.
2. Capture pacotes no ambiente com problemas.
3. Analise quais pacotes não existem na captura que reproduz o problema.

TROUBLESHOOTING DE EFEITOS COLATERAIS



Exemplo 2 de troubleshooting:

1. Tente abrir o site e diagnosticar com as ferramentas de debug do navegador qual URL exatamente não está funcionando. Exemplo:


	m=ws9Tlc,O6y8ed,aW3pY,GkRiKb,e5qF...	200	script	www.gstatic.com/...	(memory ...)	0 ms
	m=p3hmRc,LvGhrf,RqjULd	200	script	www.gstatic.com/...	8.5 kB	10 ms
	m=sOXFj,q0xTif,WNBcme	200	script	www.gstatic.com/...	10.9 kB	11 ms
	m=AZNOqf,UMu52b,EBYgl	200	script	www.gstatic.com/...	6.0 kB	9 ms
	m=P6sQOc	200	script	www.gstatic.com/...	(memory ...)	0 ms
	ListAccounts?listPages=0&authuser=0&...	200	xhr	www.gstatic.com/...	0.4 kB	414 ms
	m=Wt6vjf,hhhU8,FCpbqb,WhJnk	200	script	www.gstatic.com/...	(memory ...)	0 ms
	log?format=json&hasfast=true&auth...	200	xhr	www.gstatic.com/g...	0.2 kB	83 ms
	log?hasfast=true&auth=SAPISIDHASH+...	200	ping	www.gstatic.com/...	0.2 kB	79 ms
	log?hasfast=true&auth=SAPISIDHASH+...	200	ping	www.gstatic.com/...	0.2 kB	85 ms
	g1.globo.com	(failed) n...	document	Other	0.0 kB	43.91 s
	data:image/png;base	200	png	chrome-error://chrome	(memory ...)	0 ms
	data:image/p		png	chrome-error://chrome	(memory ...)	0 ms
	data:image/png;base...	200	png	chrome-error://chrome	(memory ...)	0 ms
	g1.globo.com	(pending)	document	Other	0.0 kB	Pending

40 requests | 76.4 kB transferred | 1.9 MB resources


Console AI assistance What's new x



 WWW.SAGENETWORKS.COM.BR

 [sage_networks](https://www.instagram.com/sage_networks)

 [Sage Networks](https://www.linkedin.com/company/sage-networks)

 +55 (19) 3500-6269