SAGE NETWORKS

Utilizando

BGP Flowspec

para mitigar ataques DDoS

Daniel Damito
Thiago Ayub

O que a Sage Networks faz?

Consultoria e assessoria para Sistemas Autônomos em redes e especializada em **mitigação de 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.

E o que são ataques DDoS?

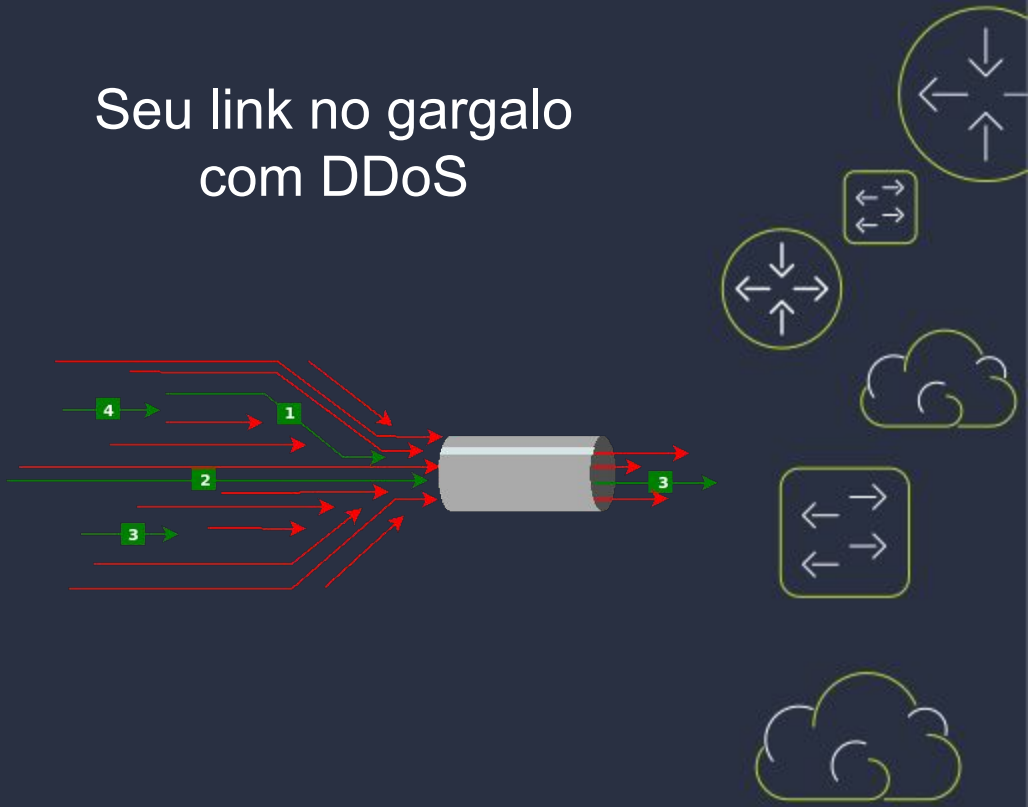
São ataques a redes dos ISPs e data centers que tem como objetivo deixá-las fora do ar ou com performance severamente degradada.

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

O que é um ataque DDoS

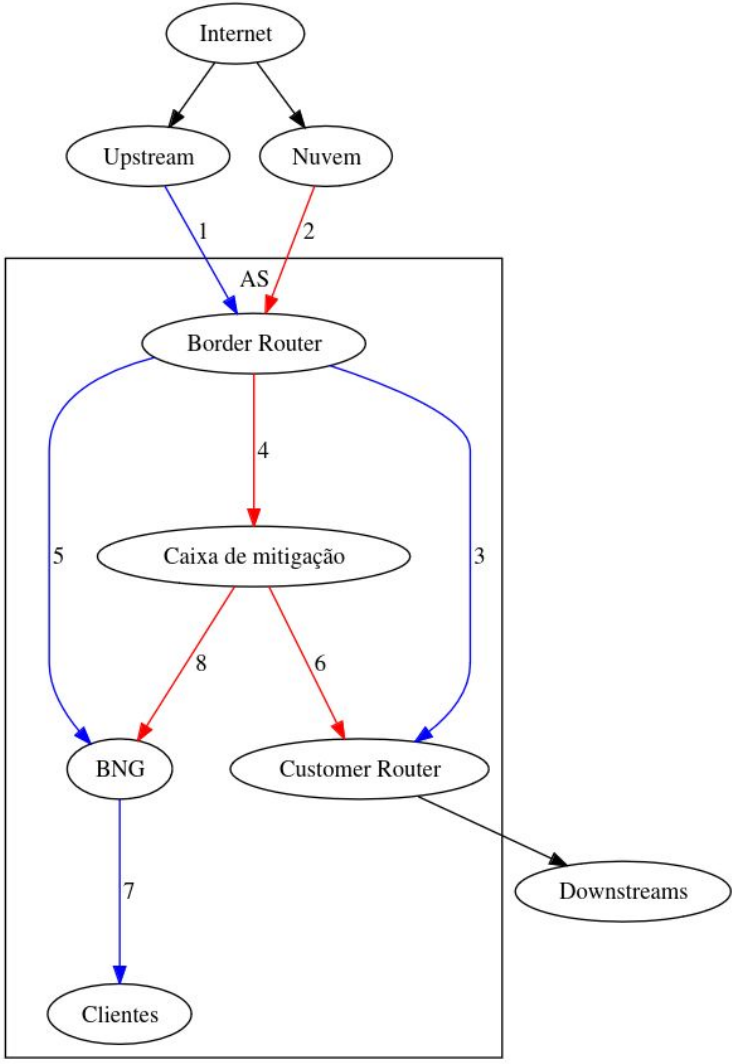
Um cano entupido
com sujeira

Seu link no gargalo
com DDoS



Possibilidades de mitigação

- Equipamentos locais (*on premise*)
  - *Inline* ou **out of band**
- Nuvem de mitigação
- Estratégia híbrida



- **Pares e azuis**: caminho normal.
- **Ímpares e vermelhos**: caminho da mitigação

Como identificar um ataque DDoS?

- Monitoramento por **gráficos** de interfaces com *upstreams*, *downstreams* e *peers* (PNI e IX) procurando por picos de banda ou pacotes por segundo.
- Monitoramento de **CPU** de servidores e *software based routers*.
- Analisar a captura de pacotes através de ferramentas como o **Wireshark**.

Como identificar um ataque DDoS?

Como identificar de forma automática?

- Roteadores e switches costumam ter suporte a protocolos de telemetria como NetFlow, sFlow e IPFIX.

Uma origem **+** Um destino **+** Um protocolo **=** **flow**

- Estes protocolos são do tipo ***push***.
- Usualmente são transportados por **UDP** e podem perder pacotes por congestionamento.
- Dados são enviados por amostragem (***sampling***)

Como identificar de forma automática?

- Roteadores e switches costumam ter suporte a protocolos de telemetria como NetFlow, sFlow e IPFIX.

Uma origem **+** Um destino **+** Um protocolo **=** **flow**

Start	Duration	Proto	Src IP Addr:Port	Src IP Addr:Port	Packets	Bytes
2024-03…	2.11	UDP	128.66.0.1:53	128.66.3.4:1433	3	204

Como identificar de forma automática?

- É necessário um detector de DDoS que receba estes flows e interprete os dados.
  - Alarme
  - Automações
    - Black hole
    - Desvio para caixa de mitigação
    - Desvio para nuvem de mitigação
    - Anúncio BGP **Flowspec**
- Existem detectores de DDoS que geram regras de Flowspec **dinamicamente** para mitigar o ataque.

Como identificar de forma automática?

- É necessário um detector de DDoS que receba estes flows e interprete os dados.
  - Alarme
  - Automações
    - Black hole
    - Desvio para caixa de mitigação
    - Desvio para nuvem de mitigação
    - Anúncio BGP **Flowspec**
- Existem detectores de DDoS que geram regras de Flowspec **dinamicamente** para mitigar o ataque.

BGP Flowspec dinâmico

- É necessário observar se a solução escolhida suporta:
  - Expirar a regra Flowspec em um **tempo** customizado.
  - Quais **verbos** são suportados (ex.: rate-limit).
  - Se é possível fazer ***white list*** de origem, destino e protocolo.
  - Se é possível limitar a quantidade de regras **simultâneas**.

Disclaimer

Quando aqui citamos sobre bugs, problemas, limitações e dificuldades encontradas, entenda que isso pode ter acontecido em versões e modelos específicos de roteadores, não sendo uma verdade absoluta para todos os cenários.

Sendo assim, sempre leiam a documentação, homologuem e testem o Flowspec em seus ambientes.

O que é o Flowspec

É uma extensão, família do protocolo BGP, que permite o envio de regras de filtragem de tráfego por BGP.

São como se fossem regras de firewall, mas distribuídas via BGP.

Veja no próximo slide um exemplo e uma comparação.

O que é o Flowspec

Uma regra de BGP Unicast é semelhante à isso:

DST: 2001:DB8::2
Next-hop: 2001:DB8:A:B::1
Community: 65535:123

Uma regra de Flowspec é semelhante à isso:

DST: 2001:DB8::2
DST-PORT: 80
Protocol: 6
Action: Deny

Flowspec vs Blackhole (RTBH)

Blackhole é uma medida drástica e inespecífica. Basicamente descarta **todo** o tráfego com destino à um IP.

Ela é eficaz em conter o dano maior de um ataque quando os alvos dos ataques são poucos ou endereços pouco importantes. Porém, em ataques de carpet bombing ou quando os destinos são endereços relevantes, o RTBH aumenta o problema.

Imagine uma blackhole no servidor de DNS do ISP?

Imagine uma blackhole em **todos** os endereços que tua empresa tem?

Flowspec vs Blackhole (RTBH)

Já o Flowspec é bastante específico e é capaz de descartar o tipo de tráfego específico do ataque, sem ferir o resto do tráfego da rede.

Num ataque de NTP, por exemplo, é possível descartar todo o NTP da rede, mas manter todo o resto do tráfego funcionando normalmente.

Limitações do Flowspec

O Flowspec é semelhante à regras de firewall de camada 4. Ou seja, ele é capaz de dar match nos critérios estabelecidos por você. Caso sua regra não seja capaz de distinguir o ataque do tráfego legítimo, ambos serão descartados.

O Flowspec também (ainda) não é capaz de dar match no payload do pacote. Existem trabalhos em andamento para isso.

Mais exemplos de regras

SRC: 2001:DB8::2
DST-PORT: 53
Protocol: 17 (UDP)
Action: Deny

DST: 2001:DB8::2
DST-PORT: 22
Protocol: 6 (TCP)
Action: Rate-limit

Possibilidades do protocolo

A RFC 8955 descrever o protocolo com mais detalhes, mas resumirei alguns pontos aqui.

Uma regra de Flowspec é composta por **matchers + ações**.

É possível combinar diversos matchers e diversas ações numa mesma regra.

Matchers

1. Destination Prefix
2. Source Prefix
3. IP Protocol
4. Port
5. Destination Port
6. Source Port
7. ICMP Type
8. ICMP Code
9. TCP Flags
10. Packet Length
11. DSCP (Diffserv Code Point)
12. Fragment

Principais ações

1. Accept
2. Discard
3. Redirect
    a. Next-hop
    b. VRF
4. Rate-limit

Principais operadores

1. == (equal)
2. > (greater than)
3. >= (greater than or equal)
4. < (less than)
5. <= (less than or equal)
6. != (not equal value)

Combinações possíveis

Regra 1:
Proto: UDP
DST: 192.0.2.0/24
SRC-PORT: 53
Action: rate-limit em 50 Mbps

Utilidade: mitigar ataques de reflexão de DNS
Efeito colateral: limitar tráfego de DNS em IPv4. Entretanto IPv6 não será afetado.

Combinações possíveis

Regra 2:
Proto: TCP
DST: 192.0.2.0/24
DST-PORT: 80
Action: Discard

Utilidade: Descartar todo o tráfego de HTTP para a rede em questão.
Efeito colateral: O HTTP desta rede ficará indisponível. Se o conteúdo for acessível em HTTPs ou IPv6, poderá continuar no ar.

Combinações possíveis

Regra 3:
Proto: TCP
DST: 192.0.2.0/24
SRC-PORT: 443
TCP Flags: SYN and ACK
Action: Discard

Utilidade: Mitigar ataque de SYN+ACK para a rede em questão.
Efeito colateral: Nenhuma nova conexão em IPv4 poderá mais ser estabelecida.

Conclusões das regras anteriores

Regras 1 e 2: Poderiam surtir bons efeitos com poucos efeitos colaterais a depender do cenário.

Regra 3: Poderia resolver o ataque com um impacto tão alto quanto o do próprio ataque em si.

Mecanismo de validação

É um mecanismo complexo, o qual não me aprofundarei.

Basicamente possui duas utilidades práticas:

1. Re-utilizar a mesma lógica de filtragem aplicada no Unicast;
2. Garantir segurança das regras aceitas.

O mecanismo diz: “A regra de Flowspec só será eleita caso exista, na tabela unicast, uma regra eleita para este mesmo destino e ensinada por este mesmo neighbor.”

Cenário de exemplo (validação ativada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.99
Status: eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec: eleita!

Cenário de exemplo (validação ativada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec:

Cenário de exemplo (validação ativada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec: não eleita!

Cenário de exemplo (validação ativada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: não eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec:

Cenário de exemplo (validação ativada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: não eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec: rejeitada!

Cenário de exemplo (validação desligada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: não eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.44
Action: deny

Resultado final na tabela Flowspec:

Cenário de exemplo (validação desligada)

Tabela Unicast:

DST: 192.0.2.1
NH: 192.0.2.44
Status: não eleita

Tabela Flowspec:

DST: 192.0.2.1
PROTO: UDP
Neighbor: 192.0.2.99
Action: deny

Resultado final na tabela Flowspec: eleita!

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).
  - Erros silenciosos. Ausência de **logs**.

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).
  - Erros silenciosos. Ausência de **logs**.
  - **Dessincronia** entre control plane e forward plane.

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).
  - Erros silenciosos. Ausência de **logs**.
  - **Dessincronia** entre control plane e forward plane.
  - A family Flowspec **disputa** recurso computacional com a family unicast.

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).
  - Erros silenciosos. Ausência de **logs**.
  - **Dessincronia** entre control plane e forward plane.
  - A family Flowspec **disputa** recurso computacional com a family unicast.
  - ***Reboot*** do control plane.

Limitações e bugs do Flowspec

- Os incidentes mais graves envolvem:
  - ***Flap*** da sessão BGP que transporta o Flowspec.
  - Regras de DROP incidindo sobre o **control plane** (null = any).
  - Erros silenciosos. Ausência de **logs**.
  - **Dessincronia** entre control plane e forward plane.
  - A family Flowspec **disputa** recurso computacional com a family unicast.
  - ***Reboot*** do control plane.
  - Travamento (***freeze***) da caixa como um todo.

Limitações e bugs do Flowspec

CLOUDFLARE

The Cloudflare Blog

Email A

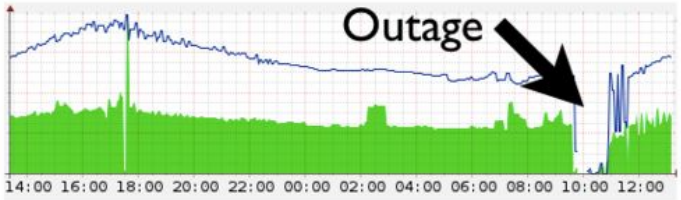
All Posts | Product News | Speed & Reliability | Security | Zero Trust | Developers | AI | Policy

Today's Outage Post Mortem

03/03/2013

Matthew Prince

5 min read



Limitações e bugs do Flowspec

```
+    route 173.X.X.X/32-DNS-DROP {
+        match {
+            destination 173.X.X.X/32;
+            port 53;
+            packet-length [ 99971 99985 ];
+        }
+        then discard;
+    }
```

Limitações e bugs do Flowspec

- Falha massiva do **AS3356** em 30/08/2020:

> Summary: On August 30, 2020 10:04 GMT, CenturyLink identified an issue to be affecting users across multiple markets. The IP Network Operations Center (NOC) was engaged, and initial research identified that an offending flowspec announcement prevented Border Gateway Protocol (BGP) from establishing across multiple elements throughout the CenturyLink Network. The IP NOC deployed a global configuration change to block the offending flowspec announcement, which allowed BGP to begin to correctly establish. As the change propagated through the network, the IP NOC observed all associated service affecting alarms clearing and services returning to a stable state.

“Globally, we saw a **3.5%** drop in global traffic during the outage, nearly all of which was due to a nearly complete outage of CenturyLink’s ISP service across the United States.” (Cloudflare)

Limitações e bugs do Flowspec

- O que fazer para suavizar estes riscos?
  - Teste suas regras Flowspec a cada **atualização** de software de seus roteadores.
  - Mantenha em dia a anuidade do **suporte** especializado do fabricante. Você vai precisar!
  - Faça ***bug report*** detalhados para seu fabricante e exija o *bug fix*.
  - Obtenha o apoio de uma consultoria de redes especializada no assunto.

Ambiente

Já encontramos problemas no passado em laboratórios virtuais, portanto desta vez decidimos fazer num ambiente real.

Roteador: HUAWEI NE40E-M2K-B
Daemon BGP de Flowspec: ExaBGP
Interface gráfica do Flowspec: Wanguard

Muitas configurações e IPs serão ofuscados durante a exibição do laboratório.

Flowspec

Demonstração prática

Ambiente

Já encontramos problemas no passado em laboratórios virtuais, portanto desta vez decidimos fazer num ambiente real.

Roteador: HUAWEI NE40E-M2K-B
Daemon BGP de Flowspec: ExaBGP
Interface gráfica do Flowspec: Wanguard

Muitas configurações e IPs serão ofuscados durante a exibição do laboratório.

Criando uma regra estática

system-view

flow-route name ipv6

if-match destination 2001:12ff:0:4::6 128

if-match protocol equal 58

apply deny

Criando filtros BGP

route-policy WANGUARD.IN permit node 10

route-policy WANGUARD.OUT deny node 10

Estabelecendo sessões BGP

bgp 1234

peer 10.200.91.2 as-number 1234

peer 10.200.91.2 description Wanguard

peer 2001:DB8::2 as-number 1234

peer 2001:DB8::2 description Wanguard-IPv6

Estabelecendo sessões BGP

```
## Configurações Unicast IPv4 ##

 ipv4-family unicast

  peer 10.200.91.2 enable

  peer 10.200.91.2 route-policy WANGUARD.IN import

  peer 10.200.91.2 route-policy WANGUARD.OUT export
```

Estabelecendo sessões BGP

Configurações Unicast IPv6

ipv6-family unicast

peer 2001:DB8::2 enable

peer 2001:DB8::2 route-policy WANGUARD.IN import

peer 2001:DB8::2 route-policy WANGUARD.OUT export

Estabelecendo sessões BGP

Configurações Flowspec IPv4

ipv4-family flow

peer 10.200.91.2 enable

peer 10.200.91.2 advertise-community

Estabelecendo sessões BGP

Configurações Flowspec IPv6

ipv6-family flow

peer 2001:DB8::2 enable

peer 2001:DB8::2 advertise-community

peer 2001:DB8::2 validation-disable

Demonstrações

Bloqueando ICMP em IPv6

1. Checando a eficácia do bloqueio
2. Checando a regra instalada
3. Vendo mais detalhes da regra
4. Analisando as estatísticas

Demonstrações

Criando outros tipos de regra

1. Protocolo TCP com flags;
2. Protocolo UDP com flags de fragmento;
3. Combinações de parâmetros e como validar se trata-se de um “and” ou um “or”;
4. Regras com rate limit e conversão de unidades;

Demonstrações

Combinações possíveis, mas irracionais:

1. UDP com Flag SYN;
2. Drop de ICMPv4 (proto 1 em vez de proto 58) para endereço IPv6

Estes tipos de combinações podem causar comportamentos inesperados!

Demonstrações

Bloqueando ICMP em IPv4

1. Checando a eficácia do bloqueio
2. Checando a regra na tabela
3. Explicando o mecanismo de validação na prática
4. Vendo mais detalhes da regra aplicada
5. Analisando as estatísticas

Comandos de Flowspec p/ Huawei

Ver tabela Flowspec:
display bgp flow ipv6 routing-table
dis bgp flow routing-table

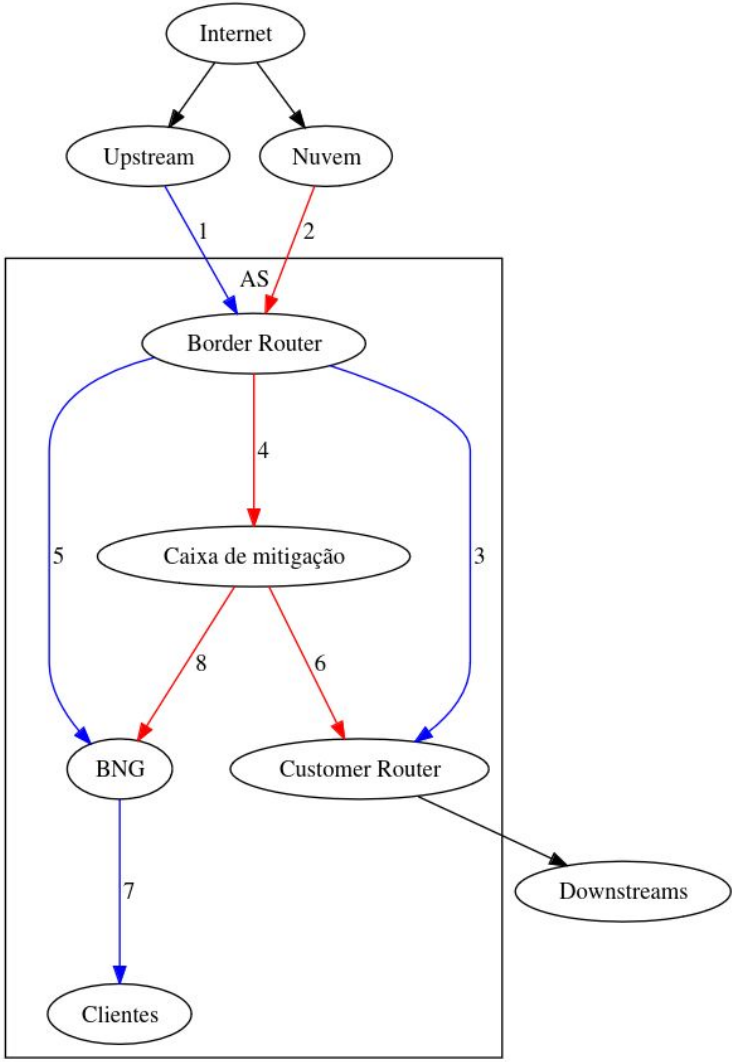
Ver uma rota específica na tabela Flowspec:
display bgp flow ipv6 routing-table $REINDEX
display bgp flow routing-table $REINDEX

Ver estatísticas de regra Flowspec:
display flowspec ipv6 statistics $REINDEX
display flowspec statistics $REINDEX

Ver estatísticas de regra Flowspec:
display bgp flow ipv6 routing-table peer 2001:DB8::2 received-routes
display bgp flow routing-table peer 10.200.91.2 received-routes

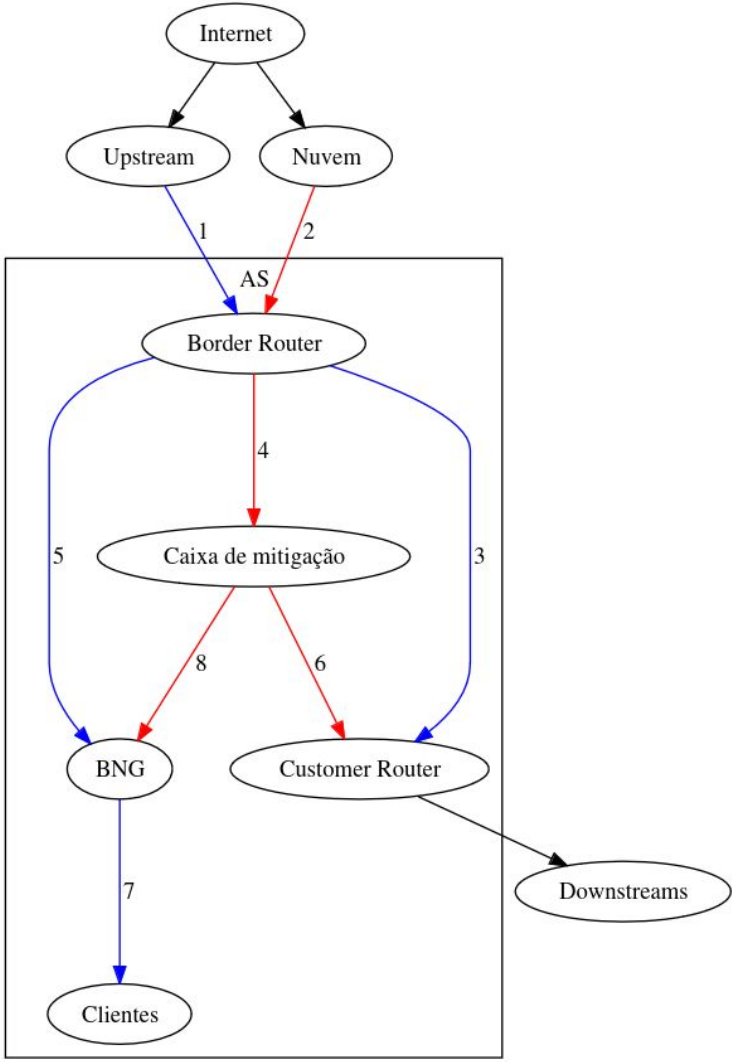
Cenários de uso do Flowspec

- Proteger **circuitos internos** de saturação causadas por ataques DDoS.


Internet
Upstream
Nuvem
1
2
AS
Border Router
4
5
3
Caixa de mitigação
8
6
BNG
Customer Router
7
Downstreams
Clientes

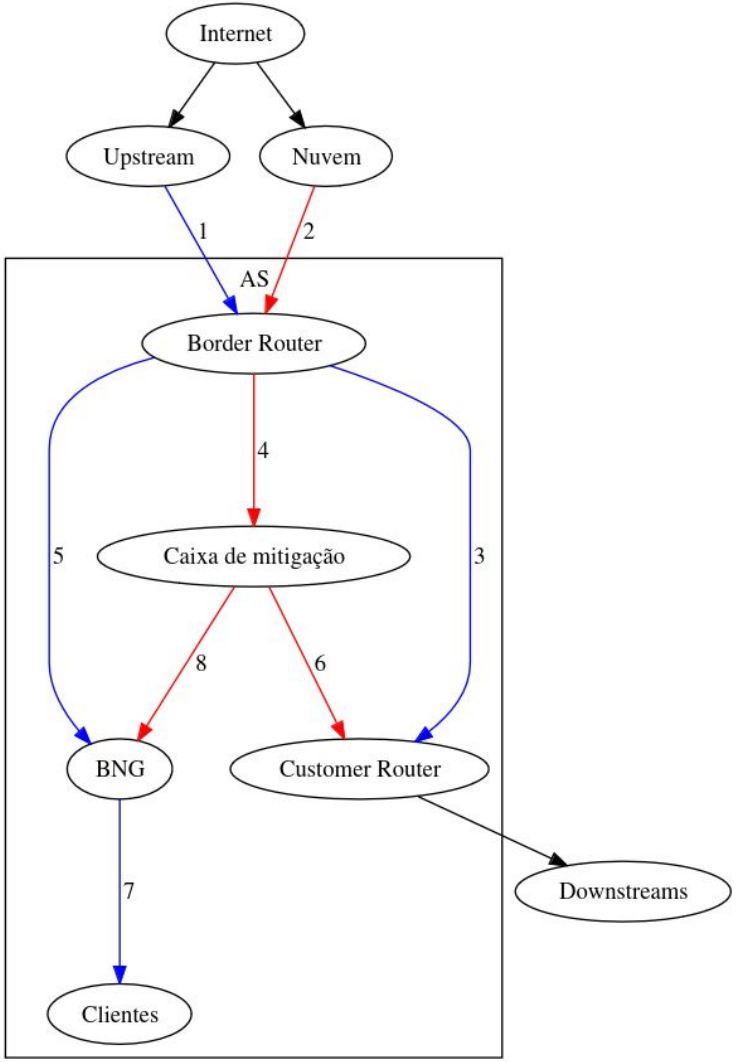
Cenários de uso do Flowspec

- Proteger **circuitos internos** de saturação causadas por ataques DDoS.
- Proteger circuitos externos de saturação ao exportar BGP Flowspec para ***upstreams***.


Internet
Upstream
Nuvem
1
2
AS
Border Router
4
5
3
Caixa de mitigação
8
6
BNG
Customer Router
7
Downstreams
Clientes

Cenários de uso do Flowspec

- Proteger **circuitos internos** de saturação causadas por ataques DDoS.
- Proteger circuitos externos de saturação ao exportar BGP Flowspec para ***upstreams***.
- **Redução** de banda (e custos) passante por caixas de mitigação.


Internet
Upstream
Nuvem
1
2
AS
Border Router
4
5
3
Caixa de mitigação
8
6
BNG
Customer Router
7
Downstreams
Clientes

Cenários de uso do Flowspec

- Proteger **circuitos internos** de saturação causadas por ataques DDoS.
- Proteger circuitos externos de saturação ao exportar BGP Flowspec para ***upstreams***.
- **Redução** de banda (e custos) passante por caixas de mitigação.
- Níveis de proteção para sistemas autônomos:
  - **Básica**: detector de DDoS + Flowspec
  - **Intermediária**: básica + Nuvem
  - **Avançada**: Intermediária + caixa de mitigação

Obrigado!

- daniel.damito@sagenetworks.com.br
- thiago.ayub@sagenetworks.com.br

- YouTube: https://www.youtube.com/@sage_networks
- Instagram: https://www.instagram.com/sage_networks/
- **Site**: sagenetworks.com.br

Telefone: (19) 3500-6269