O que é FlowSpec?

Gustavo Rodrigues Ramos
gustavo.ramos@dhc.com.br
gustavo@nexthop.com.br

Agenda

- Introdução e Motivação
- O que é FlowSpec?
- Implementação
- Verificação
- Conclusão

Introdução e Motivação

- Questões:
  - Como fazer o controle de tráfego em larga escala?
  - Como se proteger de ataques de negação de serviço?
  - Grupo de operações de redes ou grupo de segurança?
- Recente “proposed standard” do padrão FlowSpec como RFC5575 “Dissemination of Flow Specification Rules”.

http://tools.ietf.org/html/rfc5575

Ataques de Negação de Serviço: Histórico

Detecção	Contramedida
•Gráficos (MRTG) •Captura de Pacotes (sniffer) •Intrusion Detection System (IDS) •Netflow/sFlow [1] [3] •Intrusion Prevention System (IPS)	•Access-list •Firewall •Rota para Interface null0 [1] •Blackhole, sinkhole e BGP communities [2] •FlowSpec [4] [5]

[1] ftp://ftp.registro.br/pub/gts/gts07/08-ataques-datacenter.pdf
[2] ftp://ftp.registro.br/pub/gter/gter18/03-bgp-bloqueio-dos-flood.ear.pdf
[3] ftp://ftp.registro.br/pub/gts/gts0103/gts-2003-netflow-cert-rs.pdf
[4] ftp://ftp.registro.br/pub/gter/gter23/03-Flowspec.pdf
[5] http://www.nanog.org/meetings/nanog38/presentations/labovitz-bgp-flowspec.pdf

O que é FlowSpec?

- Uma forma de disseminar regras de filtros de pacotes de forma dinâmica entre roteadores que já trocam informações através do protocolo BGP.
  - Define padrões de **fluxos** (flows) e **ações** que serão aplicadas nestes fluxos.
  - Inter-AS ou Intra-AS.
  - Mecanismo de Validação.

O que é FlowSpec?

Fluxos	Ações
•Destination Prefix •Source Prefix •IP Protocol (1,6,17,…) •Port (source OR destination) •Source Port •Destination Port •ICMP Type and Code •TCP Flags •Packet Length •DSCP •Fragment	•Traffic-rate •Traffic-action •Terminal action •Sample •Redirect •Traffic Marking (DSCP)
• Suporte a IPv4.	

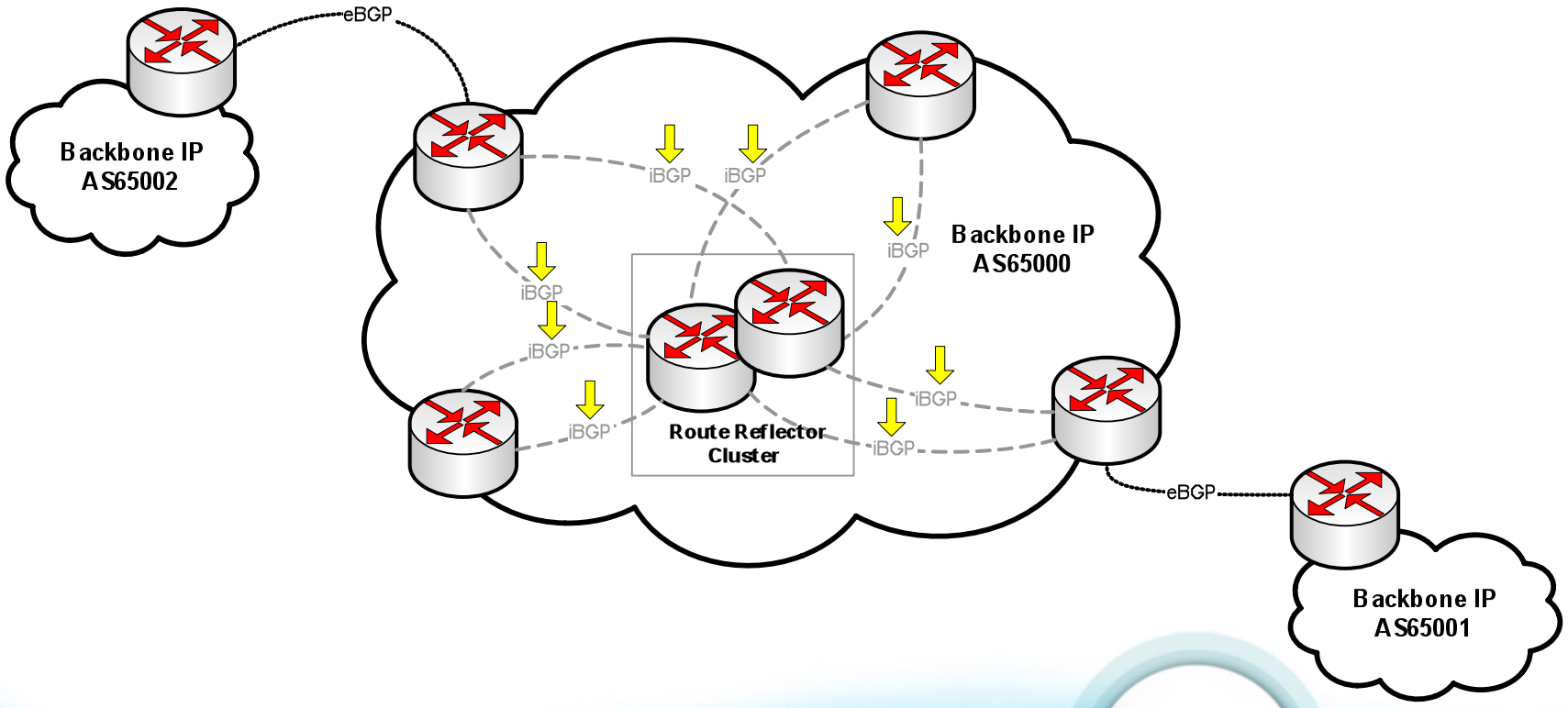
Mecanismo de Validação

- A regra de fluxo/filtragem recebida por FlowSpec para um determinado **destino**, somente será **instalada (FIB)** se foi anunciada pelo mesmo roteador/AS que anuncia a melhor rota unicast para o prefixo de destino.

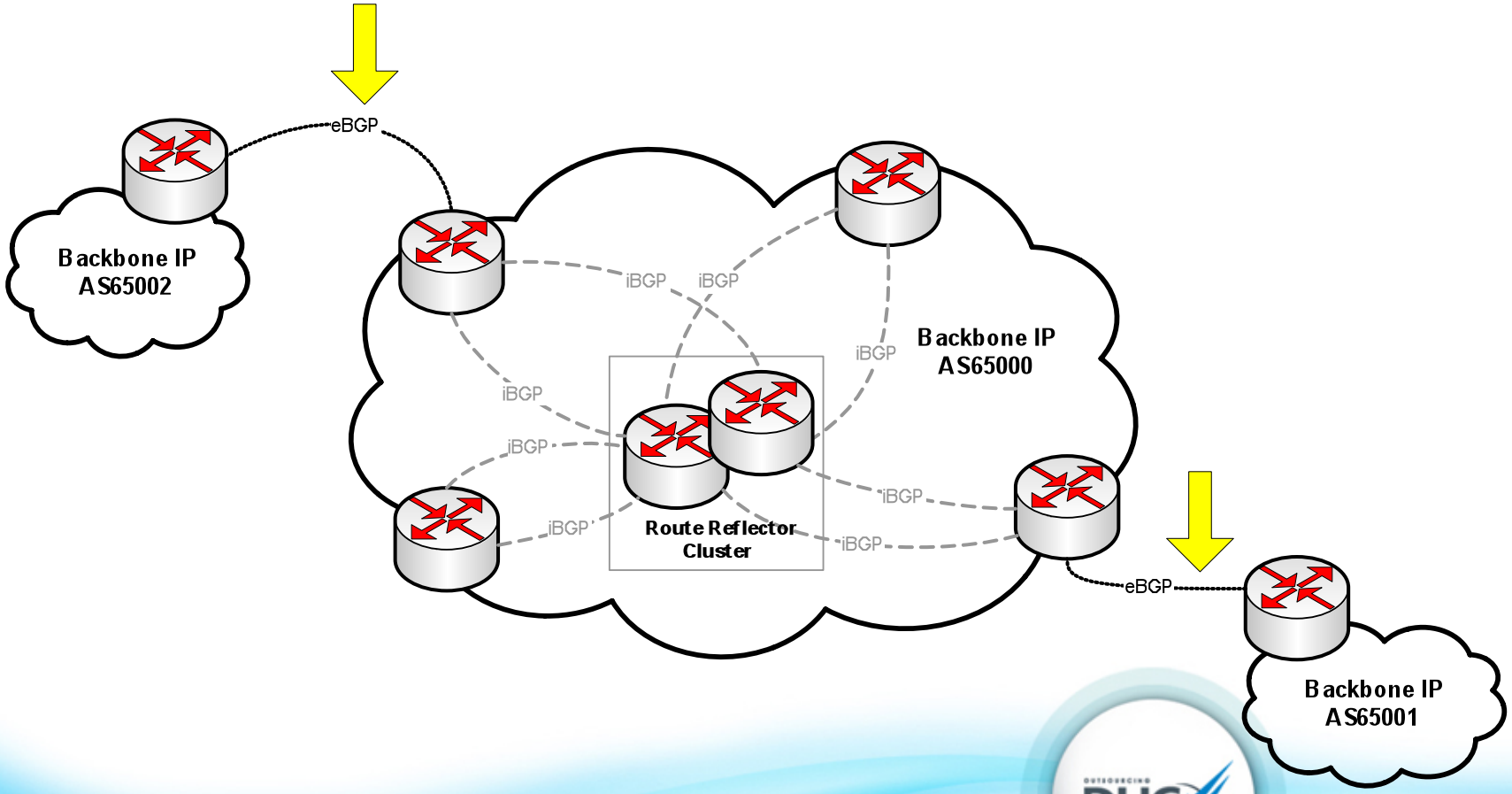
Implementação

- Plano de implementação
  - **Reserva de banda nos enlaces entre os roteadores BGP speakers (e entre os monitores da rede)**. Especialmente útil quando o ataque atravessa um enlace com menor capacidade que a banda total do ataque.
  - **Validar ou não validar?** iBGP ou eBGP?
  - **Escolha** dos roteadores ou equipamentos responsáveis por injetar as informações de filtragem (route-reflectors? IPS?).

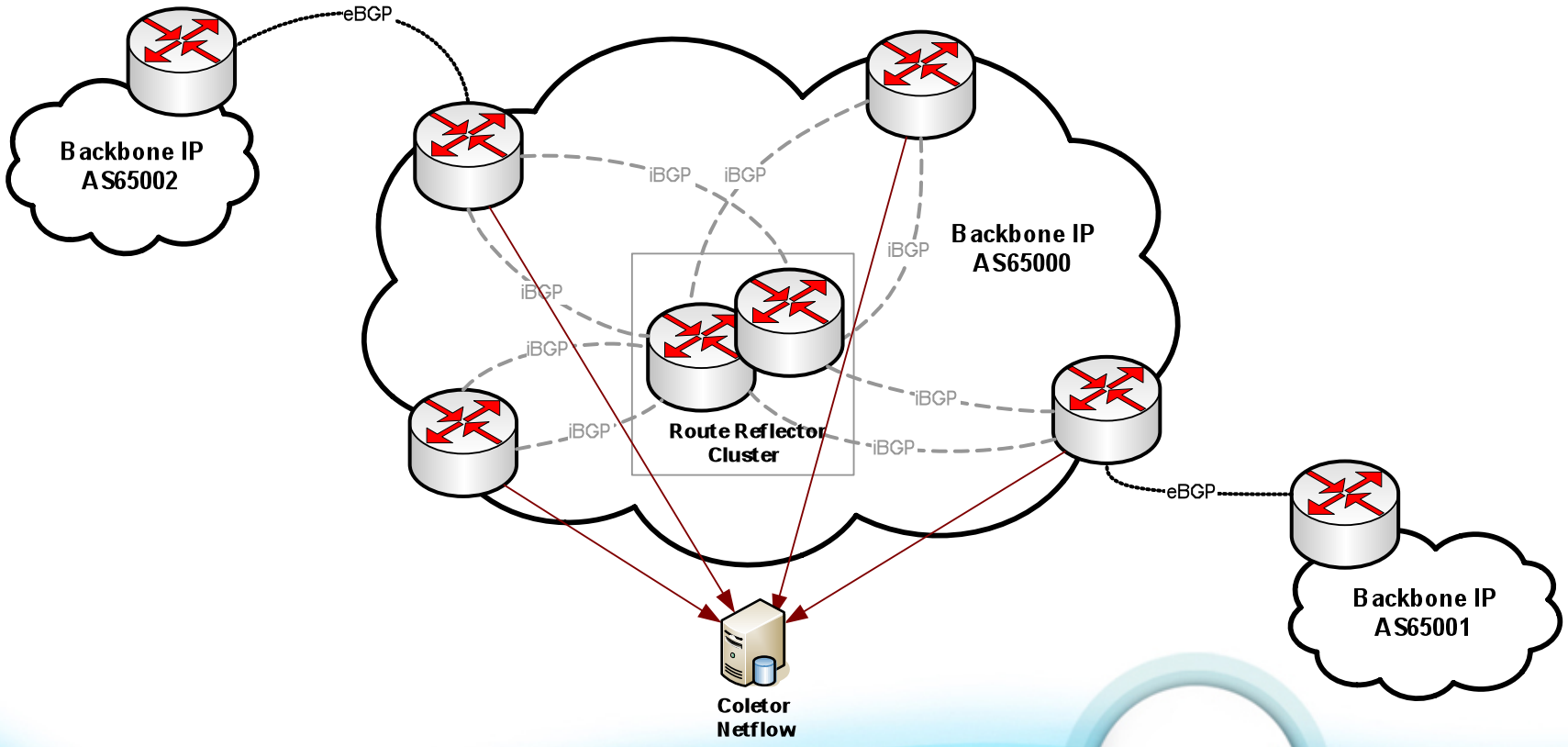
Implementação: iBGP



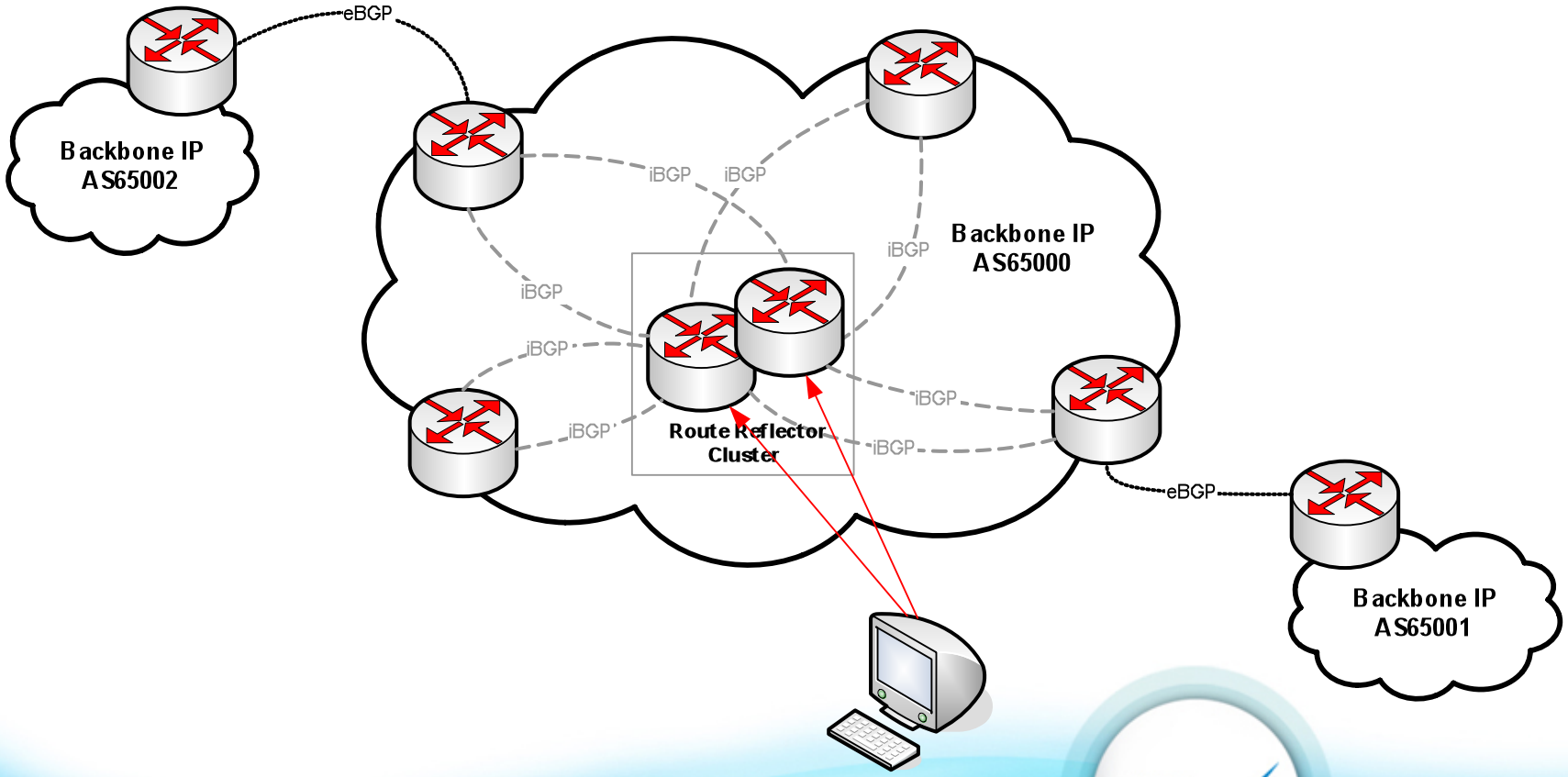
Implementação: eBGP



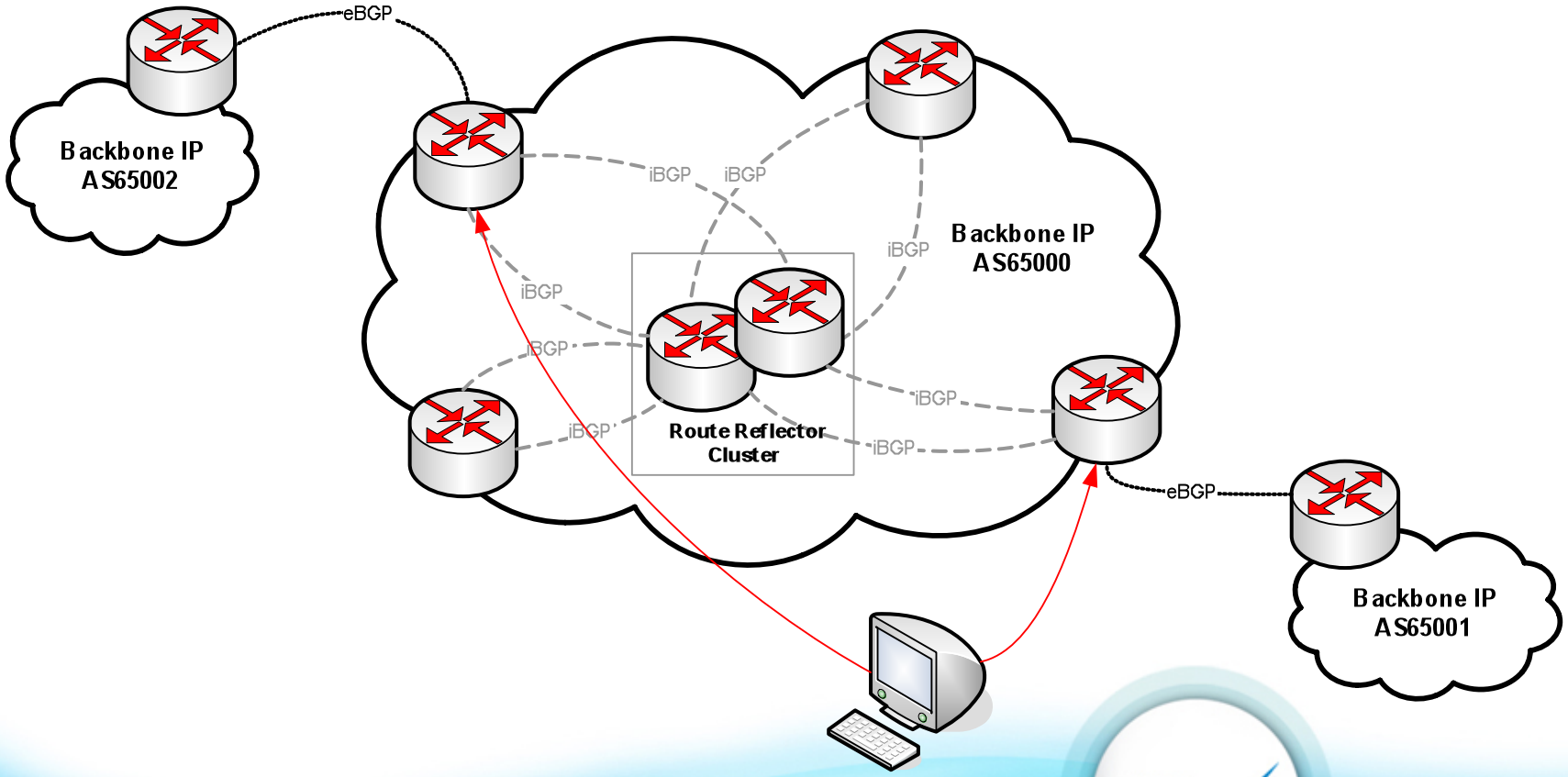
Implementação: Monitoração



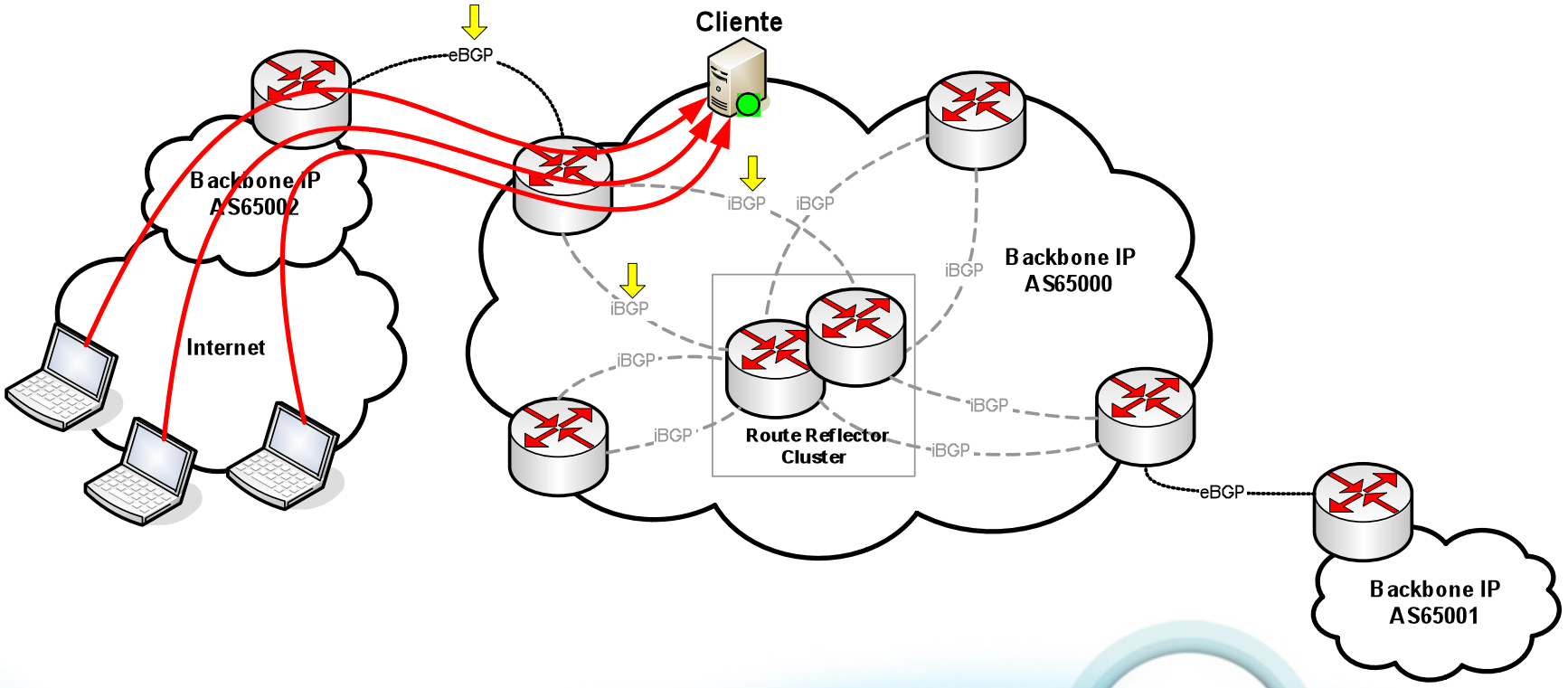
Implementação: Filtros (1)



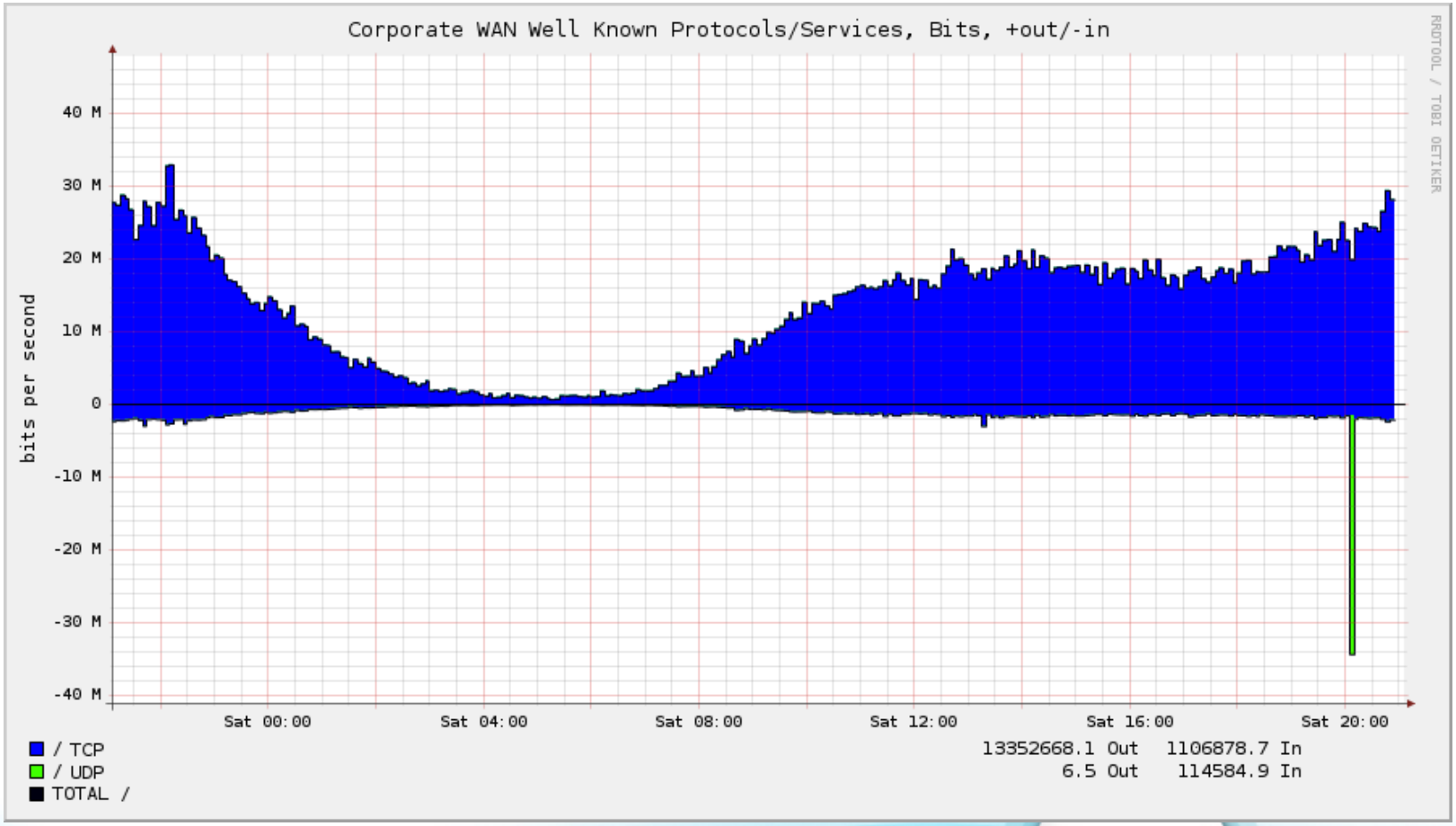
Implementação: Filtros (2)



Exemplo de Ataque



Exemplo de Ataque



Implementação

- A configuração em 3 passos.
- **Ainda** somente disponível para JunOS.

Implementação

1. Definir a Regra (flow)

```
user@router> show configuration routing-options flow
route regra1 {
    match {
        destination 200.x.x.x/32;
        protocol udp;
    }
    then {
        discard;
        sample;
    }
}
```

Além da ação “discard” pode-se configurar a ação “sample”.

Implementação

2. Configurar as Sessões BGP

```
user@router> show configuration protocols bgp group GRUPO_iBGP
type internal;
local-address 10.10.10.1;
family inet {
    flow {
        prefix-limit {
            maximum 10;
        }
        no-validate INETFLOW-SENDERS;
    }
    unicast;
}
peer-as 65000;
neighbor 10.10.10.2; …
}
```

- Opção *no-validate* utilizada nas sessões iBGP e a opção de aplicar uma policy nas regras recebidas.
- Cuidado ao incluir a "family inet flow" pois há um reset da sessão BGP.
- Definir os limites para o control-plane (prefix-limit).

Implementação

3. Exemplo de Policy

```
user@router> show configuration policy-options policy-statement INETFLOW-SENDERS
term authorized-routers {
    from neighbor [ 10.10.10.2 10.10.10.3 ];
    then accept;
}
term default {
    then reject;
}
```

Aplicar controles sobre as regras recebidas dos peers BGP.

Verificação

Verificando as sessões BGP

```
user@router> show bgp summary
Groups: 2 Peers: 5 Down peers: 0
Table         Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0          1585179     318051          0          0          0          0
inet.2                0          0          0          0          0          0
inetflow.0            3          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/Received/Accepted/Damped...
200.xxx.xx.x          65000     458051      60617       0       0  4d 0:10:21 Establ
  inet.0: 312129/318051/318051/0
  inetflow.0: 1/1/1/0
...
```

```
user@router> show route table inetflow.0

inetflow.0: 1 destinations, 3 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

200.x.x.x,*,proto=17/72
                *[BGP/170] 3d 14:54:27, localpref 100, from 200.xxx.xx.x
                  AS path: I
                  Fictitious
```

Verificação

- Texto: **show interface xe-2/3/0 extensive**
- Gráfica: MRTG, CACTI, etc. (bps ou pps).
- Ok. Não vejo mais o ataque, não há mais impacto. **Mas o ataque continua?**
  - Pode-se configurar a diretiva “sample” na regra para continuar gerando informações (e/ou coletando) de Netflow.

Verificação

Para onde foi o ataque?

user@router> **show services accounting flow-detail source-prefix 189.x.x.x/32 detail**
Service Accounting interface: sp-1/2/0, Local interface index: 129
Service name: (default sampling)
Interface state: Accounting

Protocol	Input interface	Source address	Source port	Output interface	Destination address	Destination port	Packet count	Byte count	Time since last active timeout	Packet count for last active timeout	Byte count for last active timeout
udp(17)	xe-0/0/0.xxxx	189.x.x.x	54804	xe-1/3/0.xxxx	200.x.x.x	**80**	3	168	NA	NA	NA

Conclusão

- Considerar a implementação utilizando um *único* fabricante.
- Baixo custo.
- Resposta mais rápida a incidentes (principalmente em ambientes com muitos roteadores).
- Possibilidade de filtrar os ataques mais próximo a *origem*.
- Granularidade.

Perguntas?

???

Contato:

Gustavo Rodrigues Ramos

gustavo.ramos@dhc.com.br

gustavo@nexthop.com.br