Flowspec em ação

Experiência de uso na RNP

Raniery Pontes

Junho de 2007

Intro

- Visão geral de flow specifications (flowspec)
- Necessidades da RNP no campo de "filtros dinâmicos"
- Configurando (Junos)
- Um DOS real
- Experiência de uso e aspectos operacionais

Flow specification

Uma visão geral

Delimitando o problema:

- *Foco em DDoS*
- *Objetivos: salvar a nossa infra-estrutura e idealmente proteger o cliente*
- *Práticas comumente utilizadas nos provedores tem apresentado limitações*

Algumas alternativas (?!?!):

- *Black-holes para o IP de destino: "grato por completar o meu ataque"*
- *Filtros "BGP" para o endereço de origem: complicados para o caso de um grande número de fontes e endereços forjados*
- *ACL´s: manutenção complicada e algo perigosa (especialmente sob pressão)*

Idéia básica de flow specifications

- *Usar o BGP como mecanismo de transporte de informações de filtros (flow specifications)*
- *Os roteadores que recebem essa informação aplicam os filtros imediatamente*

simples assim

Idéia básica de flow specifications

- *A ação dos roteadores não se resume à filtragem "nua e crua": é possível outras ações como limitação de banda e amostragem*
- *Definida por um draft do IETF:*

  draft-marques-idr-flow-spec-03.txt

Um pouco mais de detalhe

- *Codificar as regras de flowspec através de uma nova address family BGP (vide Multiprotocol BGP)*
- *Ações no tráfego são especificadas através de communitites especiais e incluem: filtrar (óbvio), rate-limit, amostrar, redirecionar, aceitar*

Filtrando o quê ?

- *Especificação do tráfego bem mais detalhada, através de uma combinação de:*

  prefixo de origem/destino, porta de origem/destino, tipo e código ICMP, tamanho do pacote, DSCP, flag TCP, codigo de fragmentação, etc.

Ex: filtrar tráfego UDP com origem no ip 192.168.2.3/32, com porta de destino 34675

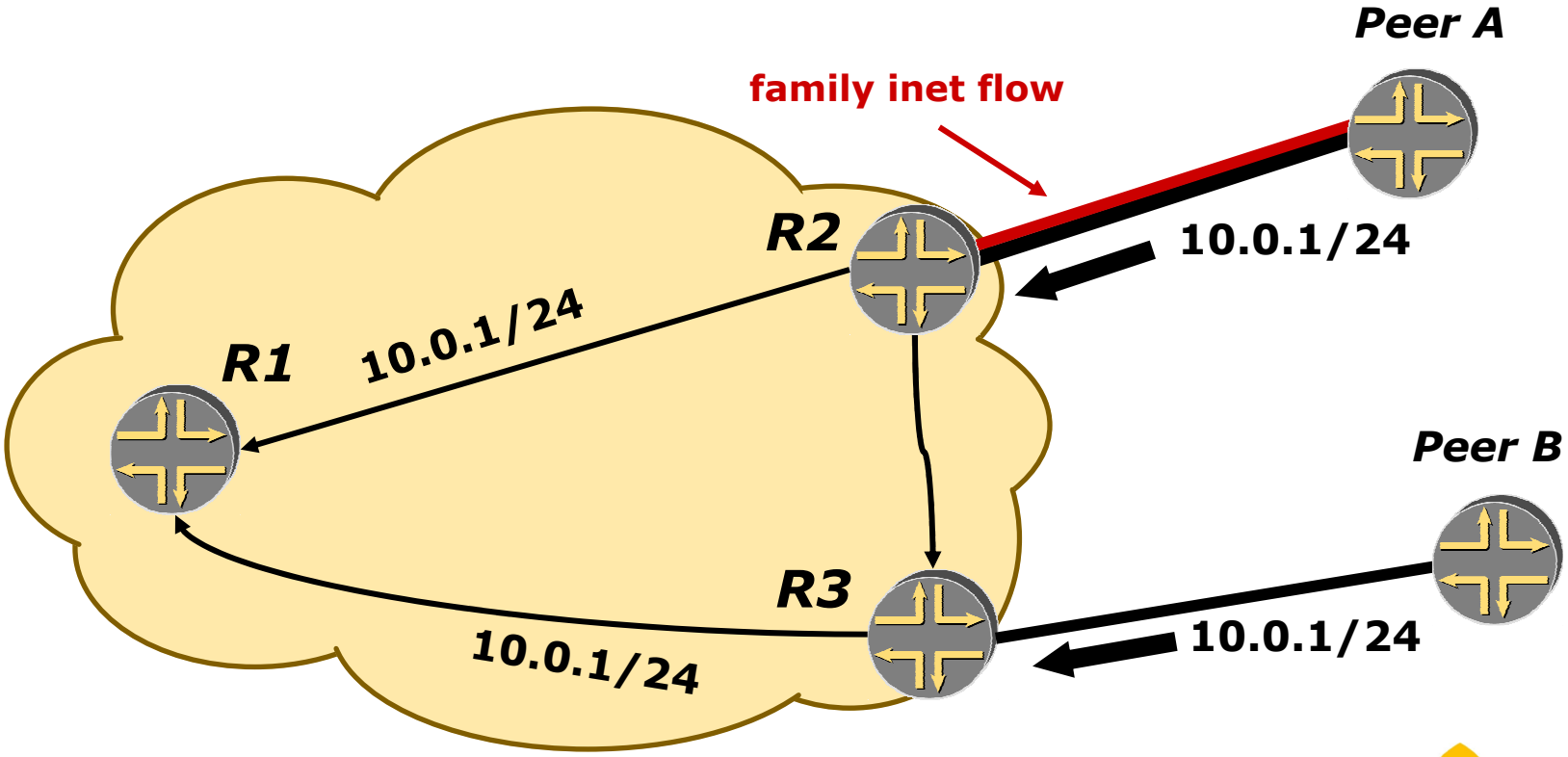
Expandindo para fora do seu AS

- *A solução é de fato intra-AS e inter-AS*
- *Embute um mecanismo de confiança/validação para que a informação possa propagar globalmente*

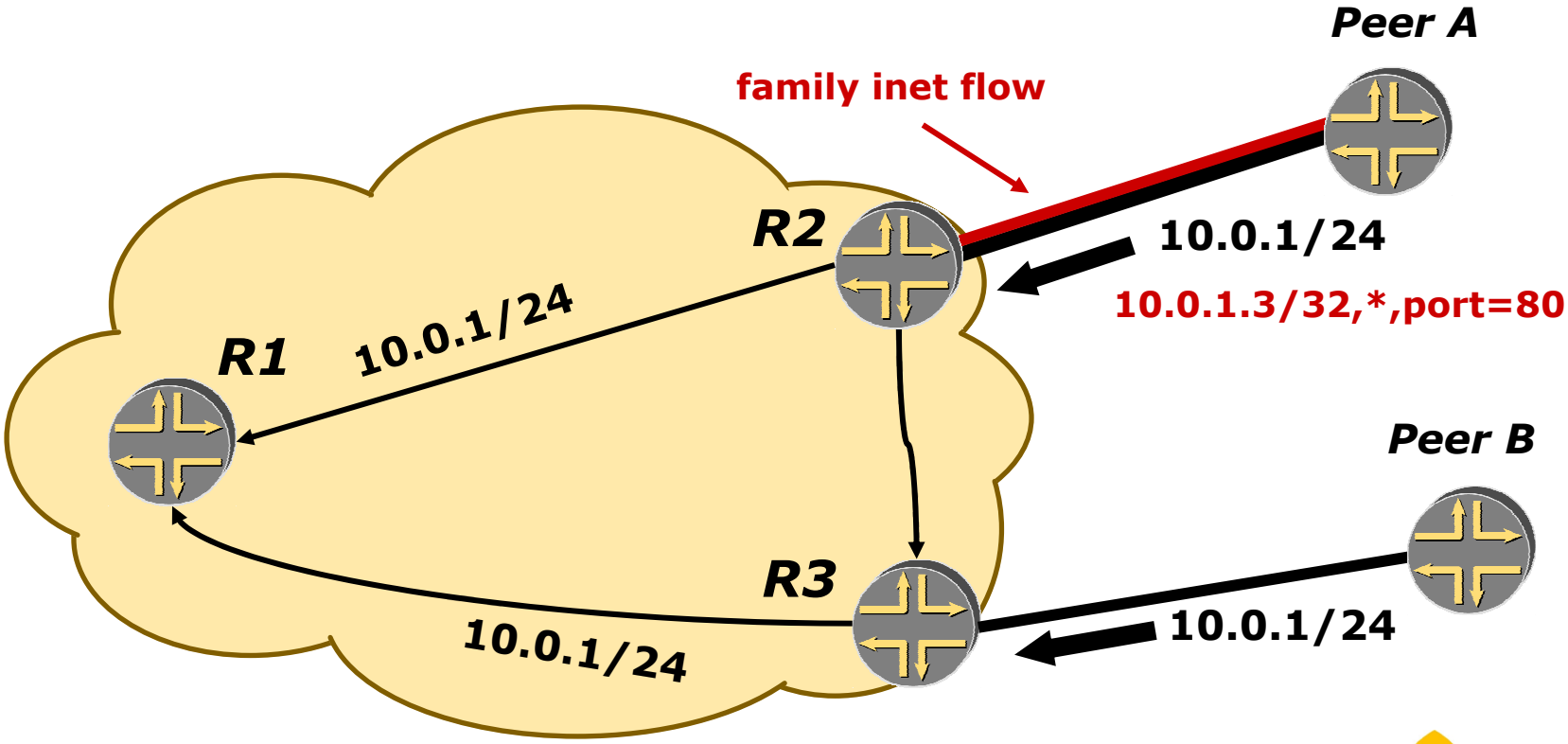
Mecanismo de validação

- *Um anúncio de flowspec será considerado válido somente se:*
- *O nó que origina a flowspec deve ser também o **mesmo** nó que origina a melhor rota unicast para o prefixo de destino*

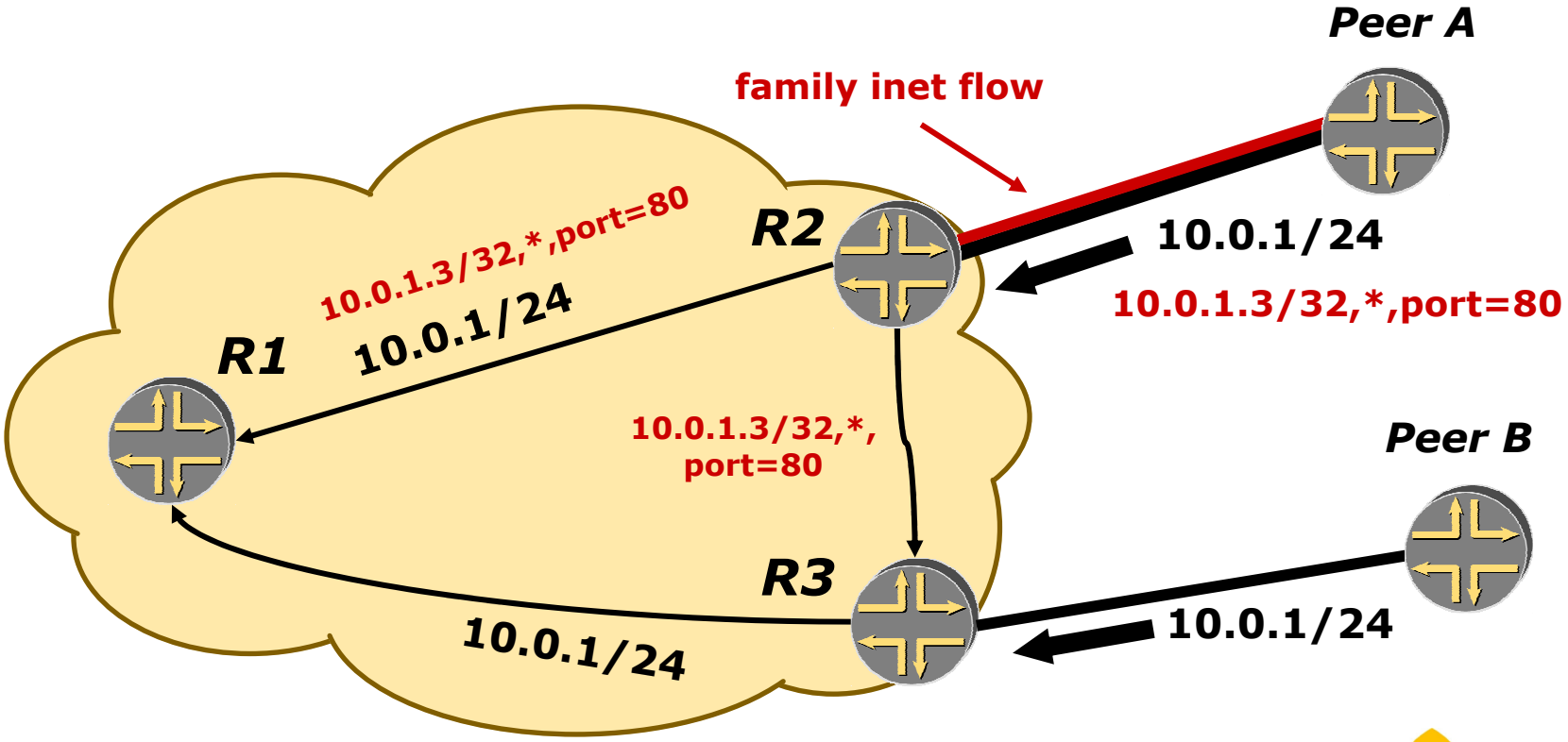
Mecanismo de validação



Mecanismo de validação



Mecanismo de validação



Anúncio flowspec: R2 aceita, R3 rejeita, R1 depende

Vantagens de usar flowspec

- *Especificação de filtros de maior granularidade*
- *Uso imediato da estrutura de BGP (interna e externa), para distribuição e validação*
- *Implementação incremental*
- *Escalabilidade e flexibilidade comprovada no MP-BGP (Multicast, IPv6, VPNs L2 e L3, VPLS)*

Limitações com flowspec

- *Somente funciona nos roteadores rodando BGP*
- *Talvez surjam questões operacionais entre o grupo de operações e de segurança*
- *Suporte nos equipamentos: Juniper ok, Cisco não (embora ambos tenham escrito o draft)*

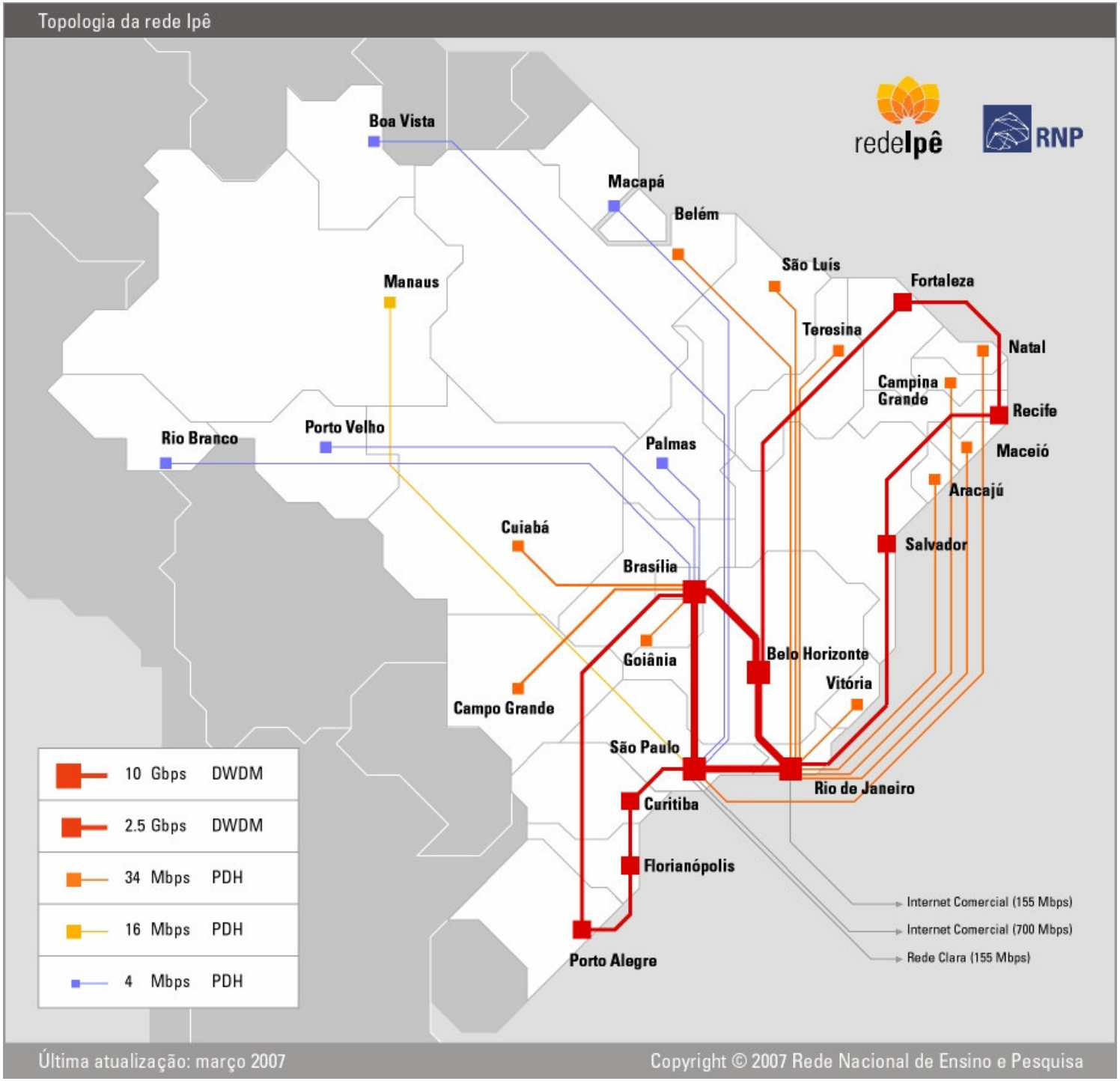
RNP e Rede Ipê

Necessidades em filtragem dinâmica

Rede Nacional de Ensino e Pesquisa - RNP

- *A RNP é responsável pela gestão da rede acadêmica nacional, atendendo centenas de universidades e institutos de pesquisa*
- *Backbone acadêmico de cobertura nacional, denominado Rede Ipê, incluindo enlaces de até 10Gbps*
- *Múltiplos peerings, ~1.5Gbps de trânsito commodity, além de ligações com a internet acadêmica*

redeIpê


Topologia da rede Ipê
redeIpê
RNP
Boa Vista
Macapá
Belém
São Luís
Fortaleza
Manaus
Teresina
Natal
Campina Grande
Recife
Rio Branco
Porto Velho
Palmas
Maceió
Aracajú
Cuiabá
Salvador
Brasília
Goiânia
Belo Horizonte
Vitória
Campo Grande
São Paulo
Rio de Janeiro
Curitiba
Florianópolis
Porto Alegre
10 Gbps DWDM
2.5 Gbps DWDM
34 Mbps PDH
16 Mbps PDH
4 Mbps PDH
Internet Comercial (155 Mbps)
Internet Comercial (700 Mbps)
Rede Clara (155 Mbps)
Última atualização: março 2007
Copyright © 2007 Rede Nacional de Ensino e Pesquisa

Necessidades usuais

- *Mitigar ataques DoS´s, direcionados ou provenientes dos nossos clientes*
- *Filtros solicitados pelo grupo de segurança (CAIS): anti-phishing são os mais comuns*

Estrutura atual

- *Migração da rede para plataforma Juniper permitiu seguir com implementação de flowspec (flow routes)*
- *Todos os roteadores com BGP configurados*
- *Propagação apenas dentro do AS (iBGP)*

Estrutura atual

- *Arquitetura muito simples, quase rudimentar ;)*
  - *Ponto central de geração de flowspecs*
  - *Alteração no mecanismo de validação via policy*

Configurando flow routes ...

Exemplos na plataforma Junos

RNP

Configuração macro de BGP

```
bgp {
    group IBGP-BACKBONE {
        type internal;
        description "Roteadores do backbone Ipe";
        family inet {
            flow {
                no-validate FLOW-ROUTE-SENDERS;
            }
            any;
        }
}
```

Configurado em todos os roteadores na malha iBGP

redeIpê

Alterando o processo de validação

```
policy-statement FLOW-ROUTE-SENDERS {
    term roteador-central {
        from neighbor a.b.c.d;
        then accept;
    }
    term last-term {
        then reject;
    }
}
```

Configurado em todos os roteadores na malha iBGP

Configurando as flow routes

```
routing-options {
    flow {
        route "CAIS#1234" {
            match {
                destination 1.2.3.4/32;
                port 80;
            }
            then discard;
        }
    }
}
```

Configurado apenas no roteador central

Observando as flow routes

```
raniery@jm320_xx> show bgp summary
Peer                     AS      InPkt      OutPkt …
10.10.10.10           1916     213712       92476 …
  inet.0: 32138/32630/0
  inet.2: 3373/3373/0
  inetflow.0: 0/0/0
20.20.20.20           1916     141653       92416 …
  inet.0: 59/19117/0
  inet.2: 1645/1645/0
  inetflow.0: 3/3/0
```

Um DOS real

Ilustrando a aplicação de flowspec

RNP

Um dia rotineiro ...

redeIpê

NFSEN - Profile live Jun 26 2007 - 04:35 - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://flows.pop-rj.rnp.br/nfsen/nfsen.php?tab=4

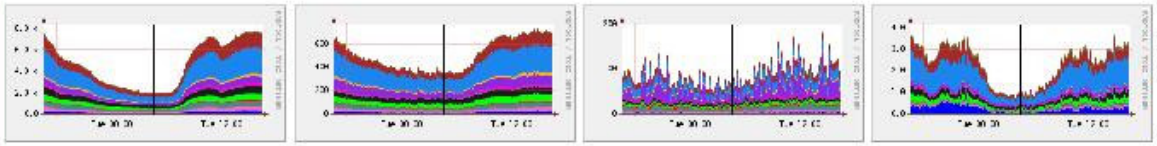
Latest Headlines | Gmail | RNP | Meu Nenê | PodcastDirectory.co... | liveCaster | evento gloria | The Evolution of Blast...

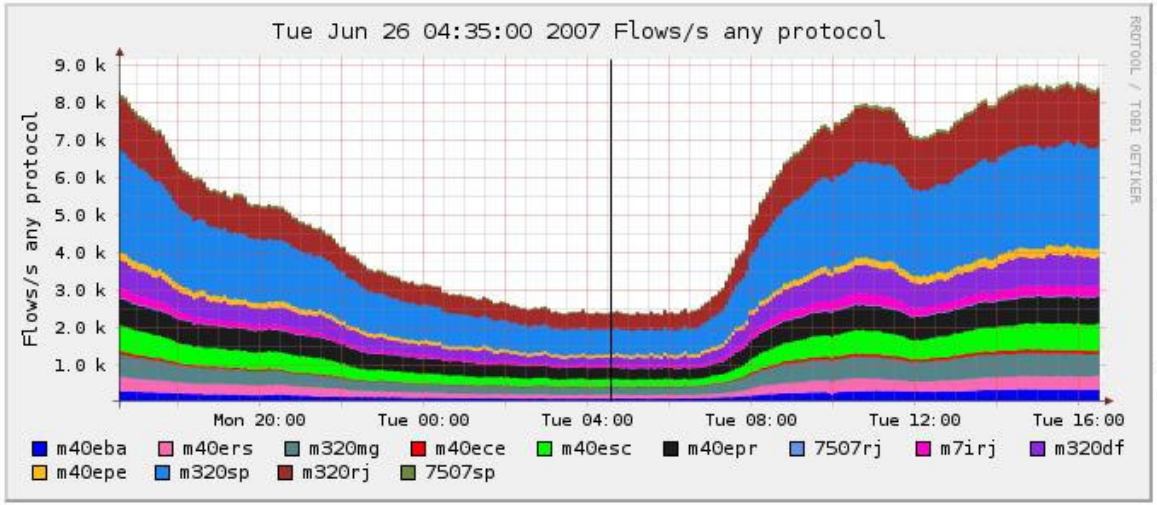
Docu | Bookmark URL | Selected Profile: live

Home | Flows | Packets | Traffic | Details | Stats | Plugins

Profile: live

TCP **UDP** **ICMP** **other**





Profileinfo:

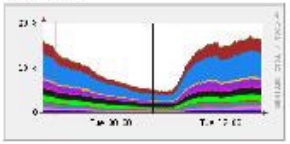
Type: continuous
Max: 50.0 GB
Exp: never
Start: Jun 23 2007 - 18:55
End: Jun 26 2007 - 16:35

t_{start} 2007-06-26-04:35

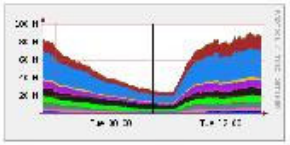
t_{end} 2007-06-26-04:35

Reset Timeslot

Packets



Traffic



Select left Mark

Display: 1 day << < | ^ > >> >|

Lin Scale | Stacked Graph
Log Scale | Line Graph

Concluído

N 2 fora 1 alerta 4 crítico AS ready

Atuando em DOS real

Oops, algo errado ...

NFSEN - Profile live Jun 22 2007 - 11:40 - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://flows.pop-rj.rnp.br/nfsen/nfsen.php

comprasnet

Latest Headlines Gmail RNP Meu Nenê PodcastDirectory.co... liveCaster evento gloria The Evolution of Blast...

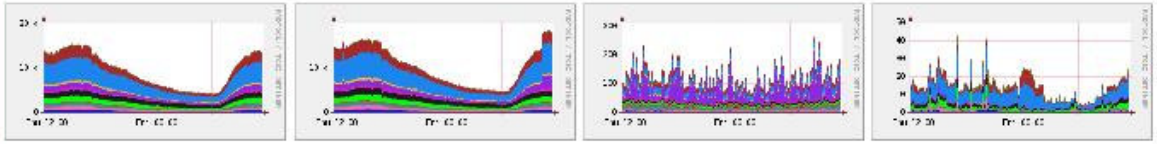
RT por alto | Listagem de Arquivos - more.gr... | CEO Wiki: HomePage | CEO Nagios | NFSEN - Profile live Jun 22 2...

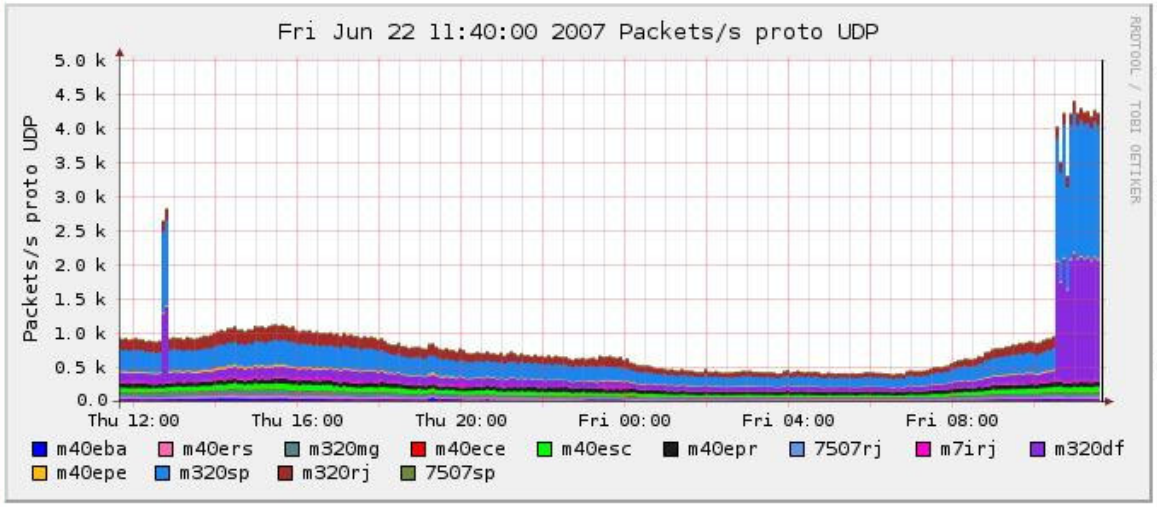
Docu Bookmark URL Selected Profile: live

Home Flows Packets Traffic Details Stats Plugins

Profile: live

TCP **any** **ICMP** **other**





Profileinfo:

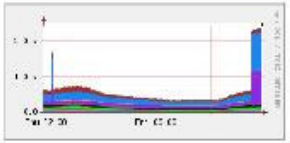
Type: continuous
Max: 50.0 GB
Exp: never
Start: Jun 20 2007 - 00:50
End: Jun 22 2007 - 11:40

t_{start} 2007-06-22-11-40

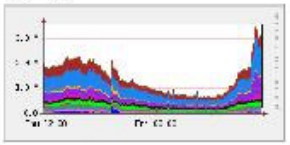
t_{end} 2007-06-22-11-40

Reset Timeslot

Flows



Traffic



Select left Mark Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Concluído 1 alerta AS ready

NFSEN - Profile live Jun 22 2007 - 11:50 - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://flows.pop-rj.rnp.br/nfsen/nfsen.php

comprasnet

Latest Headlines Gmail RNP Meu Nenê PodcastDirectory.co... liveCaster evento gloria The Evolution of Blast...

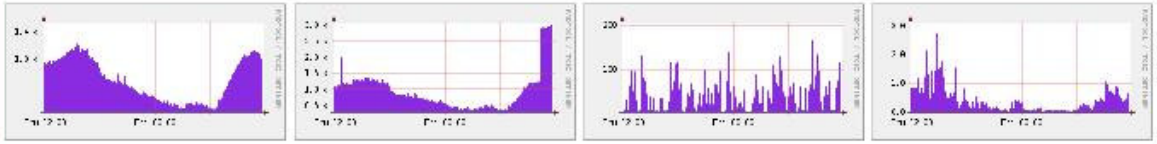
RT por alto | Listagem de Arquivos - more.gr... | CEO Wiki: HomePage | CEO Nagios | NFSEN - Profile live Jun 22 2...

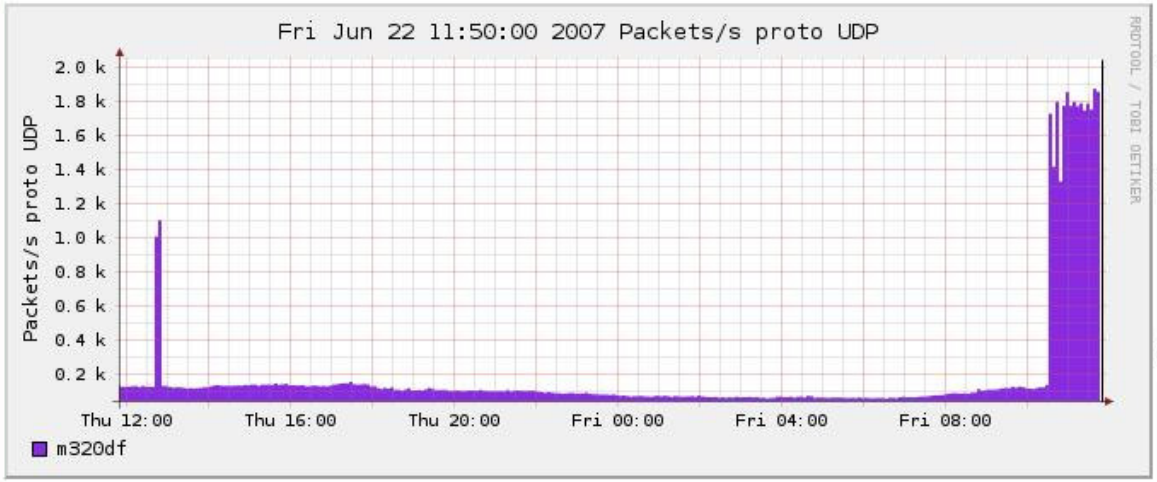
Docu Bookmark URL Selected Profile: live

Home Flows Packets Traffic Details Stats Plugins

Profile: live

TCP **any** **ICMP** **other**





Profileinfo:

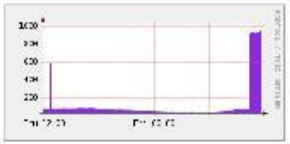
Type: continuous
Max: 50.0 GB
Exp: never
Start: Jun 20 2007 - 09:45
End: Jun 22 2007 - 11:50

t_{start} 2007-06-22-11-50

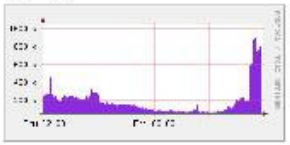
t_{end} 2007-06-22-11-50

Reset Timeslot

Flows



Traffic



Select left Mark Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Concluído Sem problemas AS ready

RNP

Identificando ...

redeIpê

Analisando o tráfego


```
nfdump  -r /usr/local/var/nfsen/profiles/live/m320_df/nfcapd.200706221140 -c 50 -a 'proto udp'

Date          flow start     Duration Proto  Src IP Addr:Port          Dst IP Addr:Port   Packets  Bytes Flows
2007-06-22 11:39:07.258    34.443 UDP    213.31.9.199:32892 ->  98.123.107.26:17966        4    116     1
2007-06-22 11:38:52.493    33.295 UDP    213.31.9.199:32892 ->  98.123.107.26:18222        2     58     1
2007-06-22 11:39:01.935    12.903 UDP    213.31.9.199:32892 ->  98.123.107.26:18734        3     87     1
2007-06-22 11:38:59.328     0.000 UDP    213.31.9.199:32892 ->  98.123.107.26:18990        1     29     1
2007-06-22 11:39:03.049     2.813 UDP    213.31.9.199:32892 ->  98.123.107.26:19246        2     58     1
2007-06-22 11:39:07.976     0.000 UDP    213.31.9.199:32892 ->  98.123.107.26:19502        1     29     1
2007-06-22 11:38:56.861    17.749 UDP    213.31.9.199:32892 ->  98.123.107.26:19758        2     58     1
2007-06-22 11:39:32.142     0.000 UDP    213.31.9.199:32892 ->  98.123.107.26:20014        1     29     1
2007-06-22 11:38:54.891    15.555 UDP    213.31.9.199:32892 ->  98.123.107.26:20270        3     87     1
2007-06-22 11:38:53.229    28.609 UDP    213.31.9.199:32892 ->  98.123.107.26:20526        3     87     1
2007-06-22 11:38:53.568     0.000 UDP    213.31.9.199:32892 ->  98.123.107.26:20782        1     29     1
2007-06-22 11:39:15.033     0.000 UDP    213.31.9.199:32892 ->  98.123.107.26:21038        1     29     1
2007-06-22 11:38:59.665    33.000 UDP    213.31.9.199:32892 ->  98.123.107.26:21294        2     58     1
(...)
```

(endereços IP anonimizados)

Aplicando a flow route

```
route Ataque-DOS-22-jun-2007 {
    match {
        destination 98.123.107.26/32;
        source 213.31.9.199/32;
        protocol udp;
        port 32892;
    }
    then discard;
}
```

RNP

Flow route aplicada ...

redeIpê

NFSEN - Profile live Jun 22 2007 - 13:55 - Mozilla Firefox

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://flows.pop-rj.rnp.br/nfsen/nfsen.php

comprasnet

Latest Headlines Gmail RNP Meu Nenê PodcastDirectory.co... liveCaster evento gloria The Evolution of Blast...

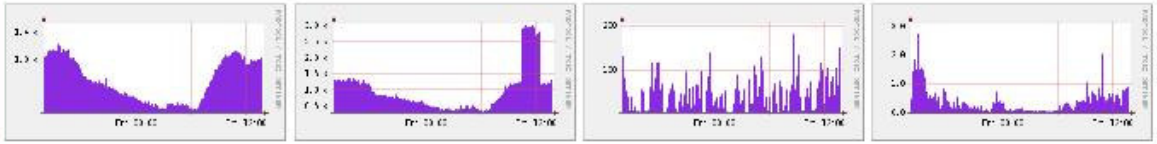
RT por alto | Listagem de Arquivos - ... | CEO Wiki: HomePage | CEO Nagios | NFSEN - Profile live Ju... | Protheus - RH Online

Docu Bookmark URL Selected Profile: live

Home Flows Packets Traffic Details Stats Plugins

Profile: live

TCP **any** **ICMP** **other**



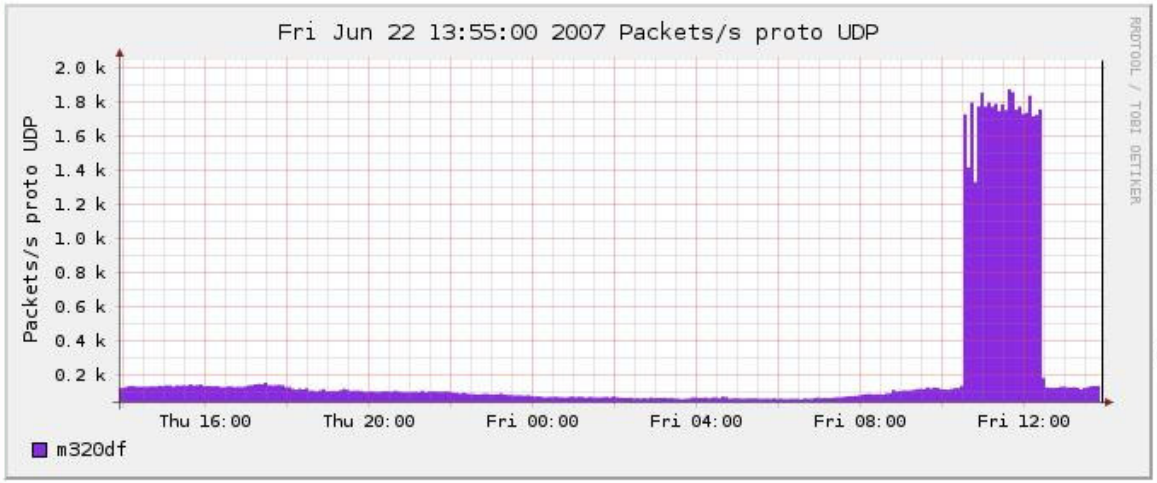
Profileinfo:

Type: continuous
Max: 50.0 GB
Exp: never
Start: Jun 20 2007 - 09:45
End: Jun 22 2007 - 13:55

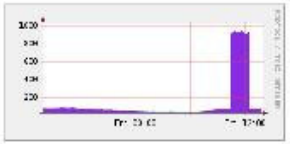
t_{start} 2007-06-22-13:55

t_{end} 2007-06-22-13:55

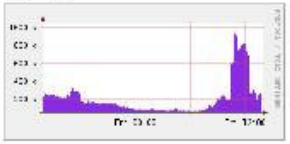
Reset Timeslot



Flows



Traffic



Select left Mark Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Concluído Sem problemas AS ready

Experiência de uso

e outros aspectos operacionais

Aspectos operacionais

- *Sem surpresas, o mecanismo tem funcionado sem problemas há mais de um ano*
- *Implementação da RNP segue a arquitetura KISS, o que obviamente ajuda ;)*

Aspectos operacionais

- *Flowspec é apenas parte da solução: precisamos avançar nos mecanismos de deteção*
  - *reclamação de cliente?*
  - *inspeção visual?*
  - *deteção automática?*

Aspectos operacionais

- *Interação entre os grupos de operações e segurança, e definição geral dos processos*
- *Filtros tradicionais via ACL´s também foram mantidos (RFC-1918, anti-spoofing). O mesmo com uRPF, quando possível*

Aspectos operacionais

- *Infelizmente ainda não é multivendor*
- *É possível uma iniciativa para habilitar flowspec entre a RNP e outros AS´s ?*

Obrigado !!!

Rede Nacional de Pesquisa

http://www.rnp.br/

Raniery Pontes

raniery@rnp.br