NetFlow para clientes do POP-RS

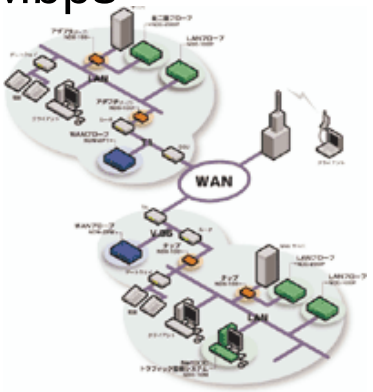
João Marcelo Ceron

Sumário

- Introdução
- Netflow
- Ferramentas Implementadas
- Relatórios Disponíveis
- Exemplos
- Conclusões

Necessidades e limitações das ferramentas atuais

- Em geral
  - RMON2
  - SNMP (estatísticas)
  - Informações básicas – falta granularidade
  - Sniffers (Ethereal, Lan Explorer, tcpdump, snort, ...)
  - Baixo desempenho para cargas acima de 10Mbps



Introdução

- Quem são os top usuários ?
  - Quanto tempo o usuário esta na rede ?
  - Qual é a porcentagem de tráfego utilizada por determinado host ?
  - Que aplicações são mais utilizadas ?
  - Engenharia de tráfego
  - Segurança

Introdução

- Quem são os top usuários ?
  - Quanto tempo o usuário esta na rede ?
  - Qual é a porcentagem de tráfego utilizada por determinado host ?
  - Que aplicações são mais utilizadas ?
  - Engenharia de tráfego
  - Segurança

Monitoramento por fluxo

- Fluxo
  - Sequência unidirecional de pacotes entre dois pontos de comunicação.
- NeTraMet: o próprio administrador define que caracteristicas seram exportadas - RFC 2123.
- NetFlow: define sete caracteristicas

Netflow

- Um padrão de exportaçaõ de fluxos desenvolvido pela CISCO.
- Disponível:
  - Roteadores Cisco
  - Roteadores Juniper
  - Roteadores Extreme
  - Plataformas *UNIX
    - Fprobe
    - Nprobe

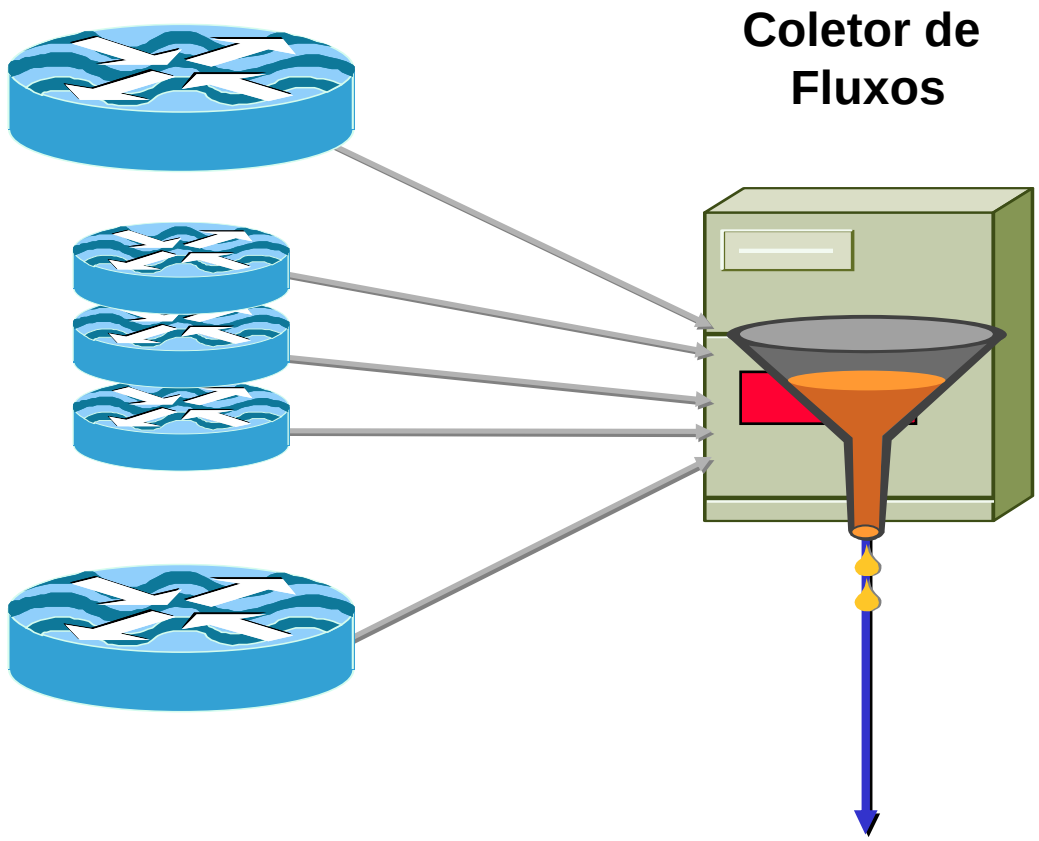
Fluxo de Informações no Netflow

Geração fluxos	Recepção de fluxos	Análise de fluxos (texto)	Geração de gráficos
• Roteadores • Switches • NTOP • Fprobe	• Flow-tools (flow-capture) • CFlowd	• Flow-tools • CFlowd • Flowscan (Top) • Console roteadores *	• RRDTool • CUFlow (cgi) Requisito: Flowscan

Netflow

- Define um tupla com:
  - IP de origem
  - IP de destino
  - Porta de Origem
  - Porta de destino
  - Tipo de Protocolo
  - TOS (Type of service)
  - Interface de entrada

NetFlow



Netflow

- Um novo fluxo é criado quando um pacote é recebido e não pertence a nenhum outro fluxo existente.
- Um fluxo expira quando:
  - Permanece inativo por mais de 15 segundos
  - Sua duração excede 30 minutos
  - Uma conexao TCP é encerrada por um FIN ou RST
  - Tabela de fluxos estiver cheia

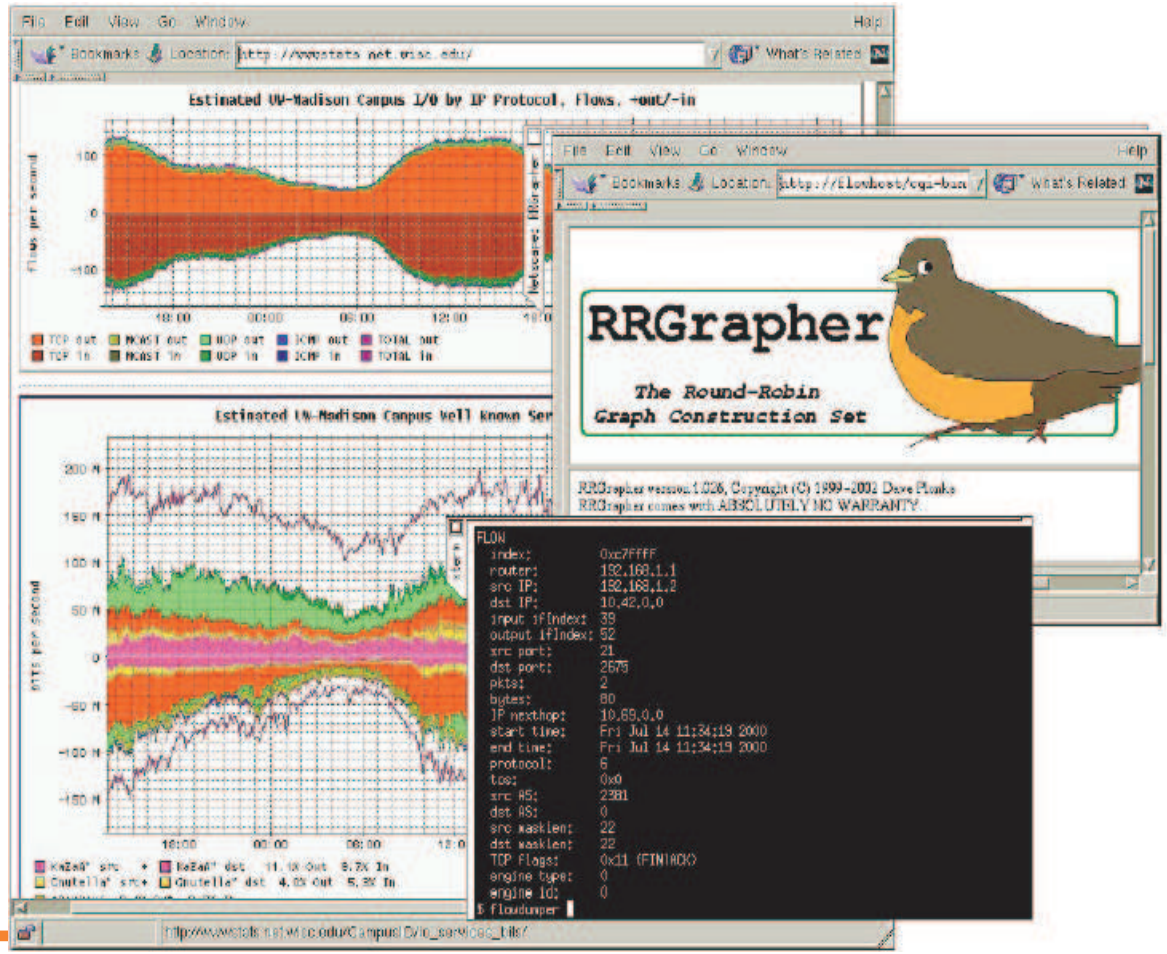
```
flow-cat ft-v05.2005-07-12.110000-0300 | flow-print  | head
```

srcIP	dstIP	prot	srcPort	dstPort	octets	packets
200.136.52.120	200.143.76.2	17	1086	53	63	1
64.233.171.85	143.54.43.36	6	80	1888	514	3
62.194.140.116	200.236.38.95	6	2808	6881	354	8
200.61.183.145	200.17.166.1	17	32768	53	72	1
61.78.58.195	143.54.9.1	17	53	53	150	1
213.186.240.98	200.236.38.47	17	11806	8777	139	1
81.244.98.204	200.18.41.61	17	9512	27264	264	3
206.190.38.231	200.160.143.212	6	80	17378	63442	47
200.233.55.228	200.233.22.106	6	2793	1433	96	2

Coleta de dados

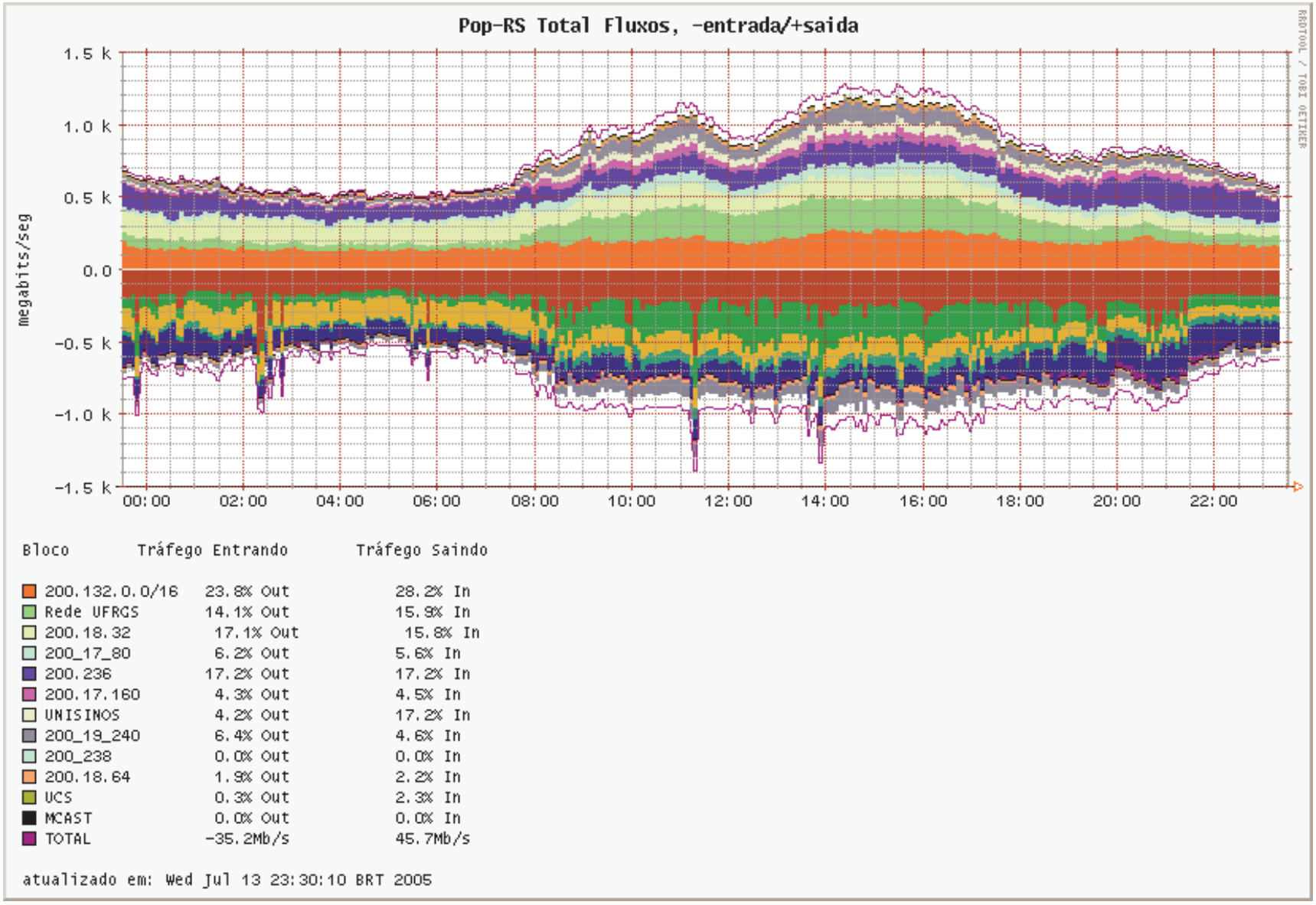
- Coleta é feita a cada 5 minutos
- 155Mbits
  - 5 minutos de coleta -> 15Mbytes*
  - Total diário -> 3,2Gbytes*
  - * dados compactados

Fluxo de Informações no Netflow



Implementação no POP-RS

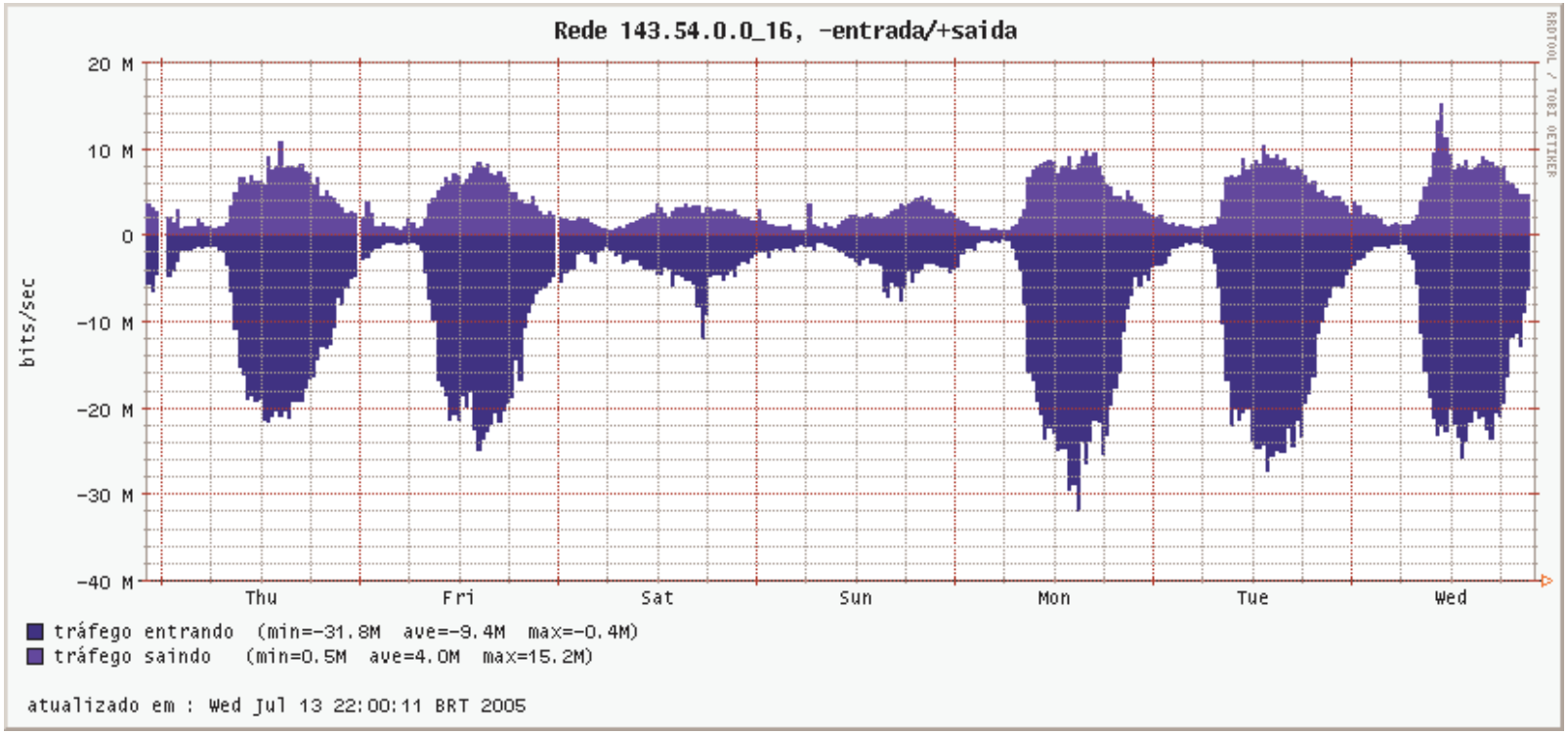
- Flowscan
  - Script Perl
  - Responsável pela geração de gráficos
  - Armazena dados em base de dados RRD
  - Gera alguns relatórios



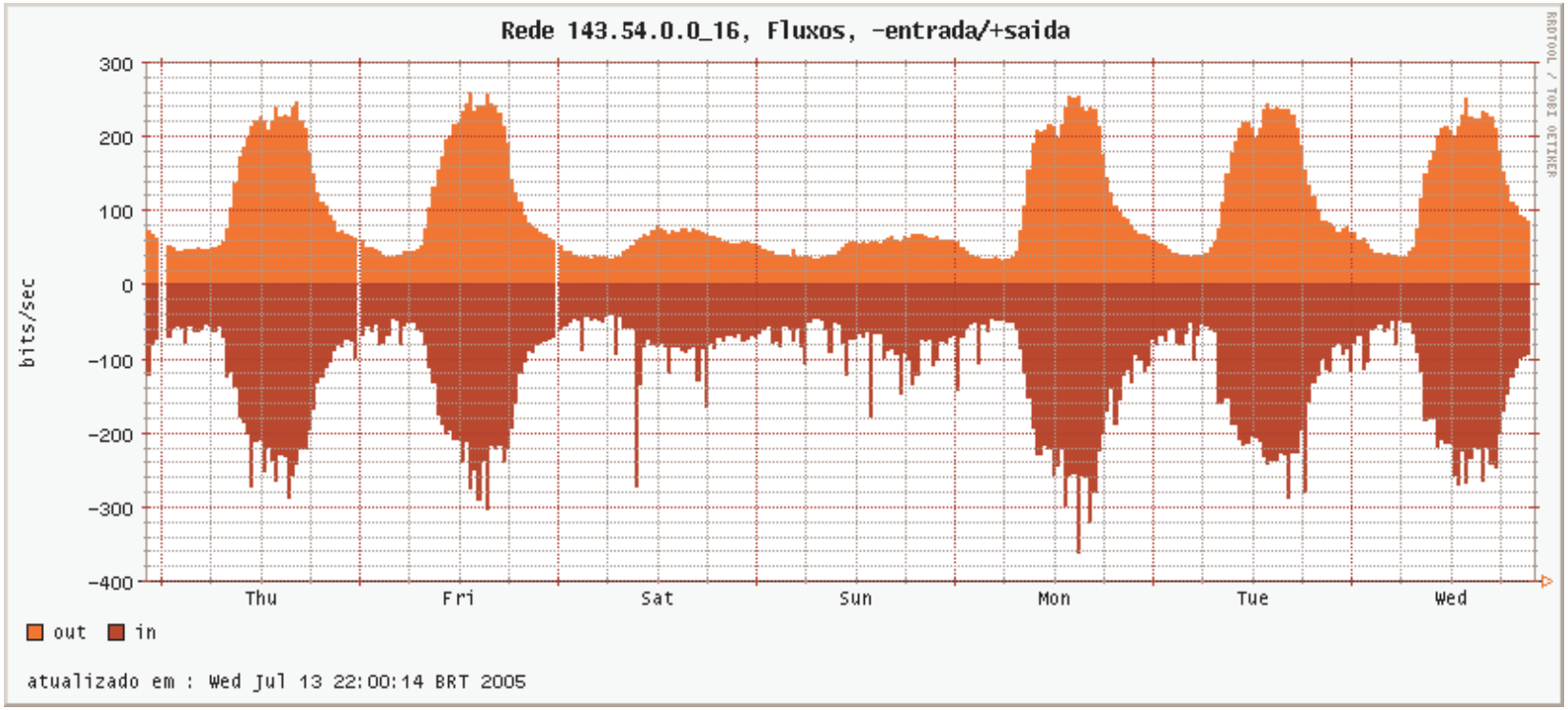
Bloco	Tráfego Entrando	Tráfego Saindo
200.132.0.0/16	23.8% Out	28.2% In
Rede UFRGS	14.1% Out	15.9% In
200.18.32	17.1% Out	15.8% In
200_17_80	6.2% Out	5.6% In
200.236	17.2% Out	17.2% In
200.17.160	4.3% Out	4.5% In
UNISINOS	4.2% Out	17.2% In
200_19_240	6.4% Out	4.6% In
200_238	0.0% Out	0.0% In
200.18.64	1.9% Out	2.2% In
UCS	0.3% Out	2.3% In
MCAST	0.0% Out	0.0% In
TOTAL	-35.2Mb/s	45.7Mb/s

atualizado em: Wed Jul 13 23:30:10 BRT 2005

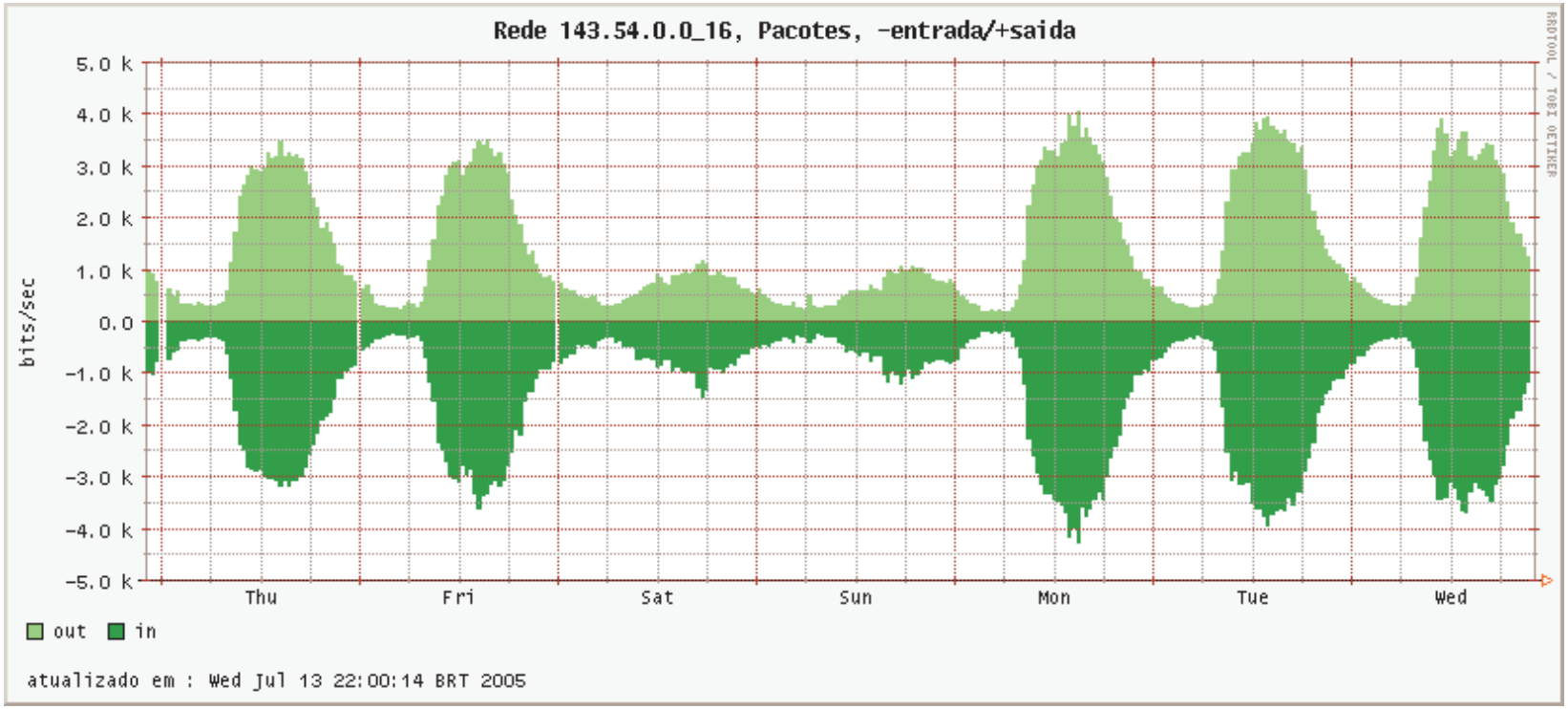
Implementação no POP-RS

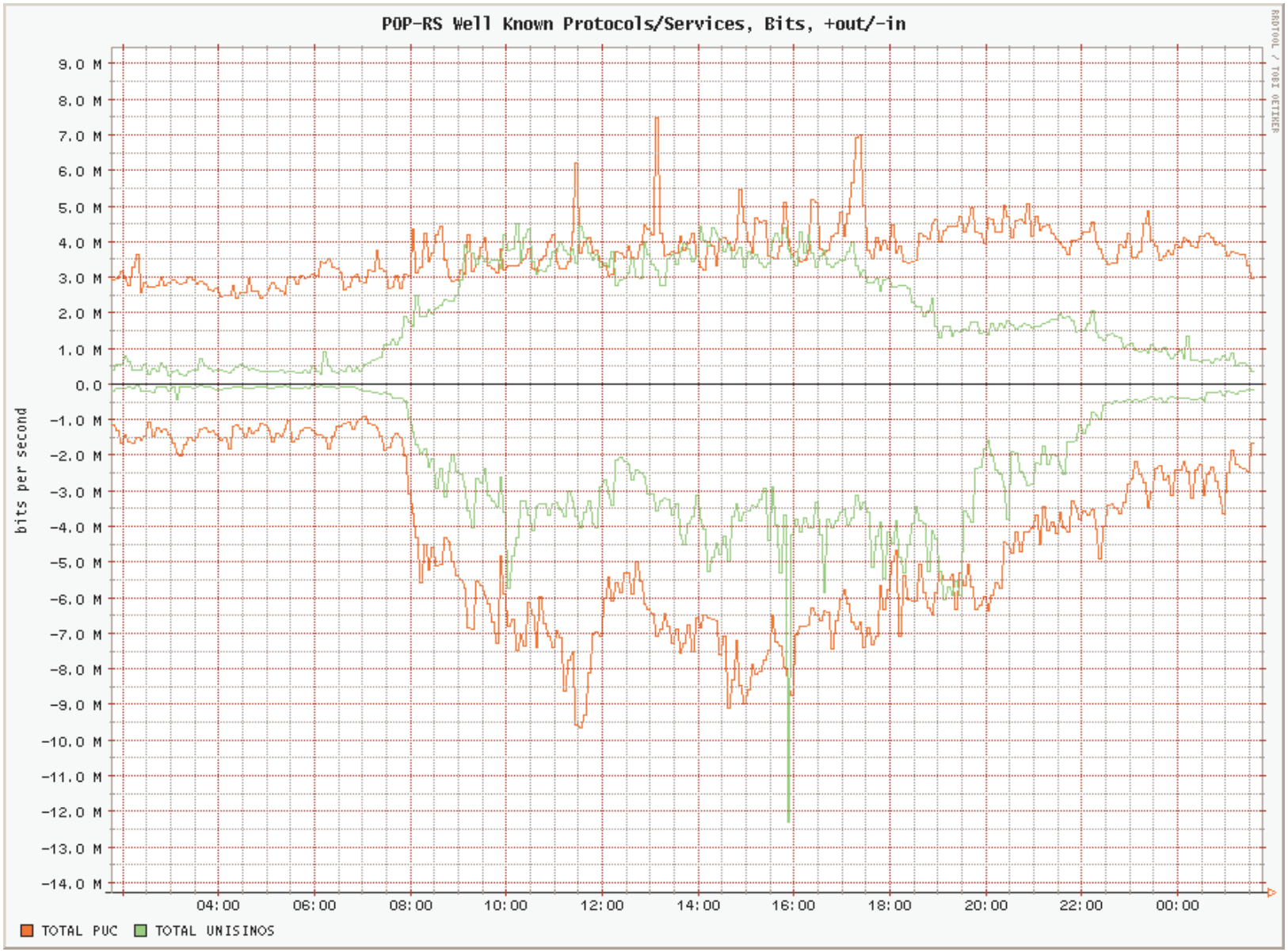


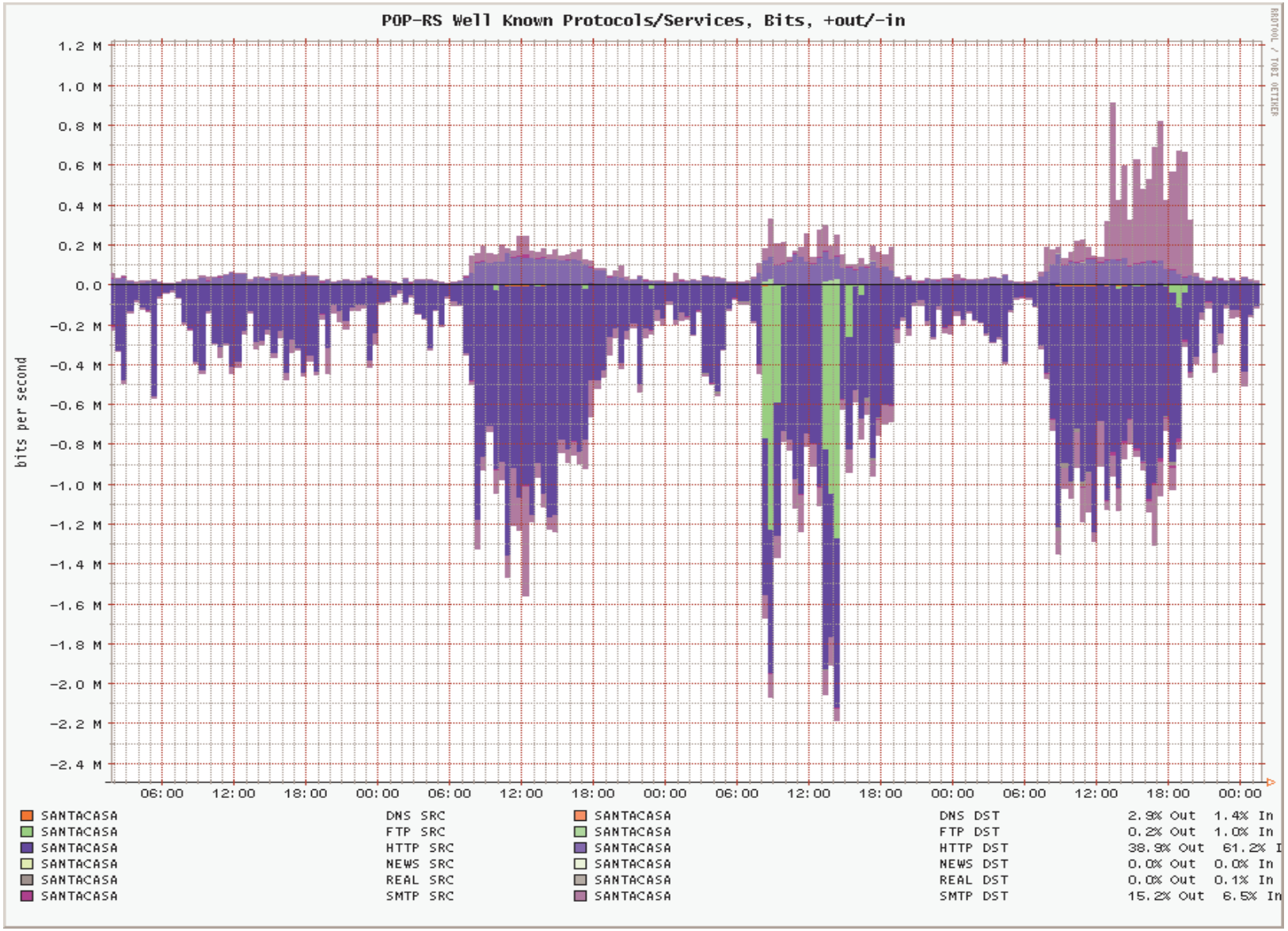
Implementação no POP-RS



Implementação no POP-RS




POP-RS Well Known Protocols/Services, Bits, +out/-in
bits per second
9.0 M
8.0 M
7.0 M
6.0 M
5.0 M
4.0 M
3.0 M
2.0 M
1.0 M
0.0
-1.0 M
-2.0 M
-3.0 M
-4.0 M
-5.0 M
-6.0 M
-7.0 M
-8.0 M
-9.0 M
-10.0 M
-11.0 M
-12.0 M
-13.0 M
-14.0 M
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
00:00
TOTAL PUC
TOTAL UNISINOS


POP-RS Well Known Protocols/Services, Bits, +out/-in
bits per second
1.2 M
1.0 M
0.8 M
0.6 M
0.4 M
0.2 M
0.0
-0.2 M
-0.4 M
-0.6 M
-0.8 M
-1.0 M
-1.2 M
-1.4 M
-1.6 M
-1.8 M
-2.0 M
-2.2 M
-2.4 M
06:00
12:00
18:00
00:00
SANTACASA DNS SRC
SANTACASA FTP SRC
SANTACASA HTTP SRC
SANTACASA NEWS SRC
SANTACASA REAL SRC
SANTACASA SMTP SRC
SANTACASA DNS DST 2.9% Out 1.4% In
SANTACASA FTP DST 0.2% Out 1.0% In
SANTACASA HTTP DST 38.9% Out 61.2% I
SANTACASA NEWS DST 0.0% Out 0.0% In
SANTACASA REAL DST 0.0% Out 0.1% In
SANTACASA SMTP DST 15.2% Out 6.5% In

Implementação no POP-RS

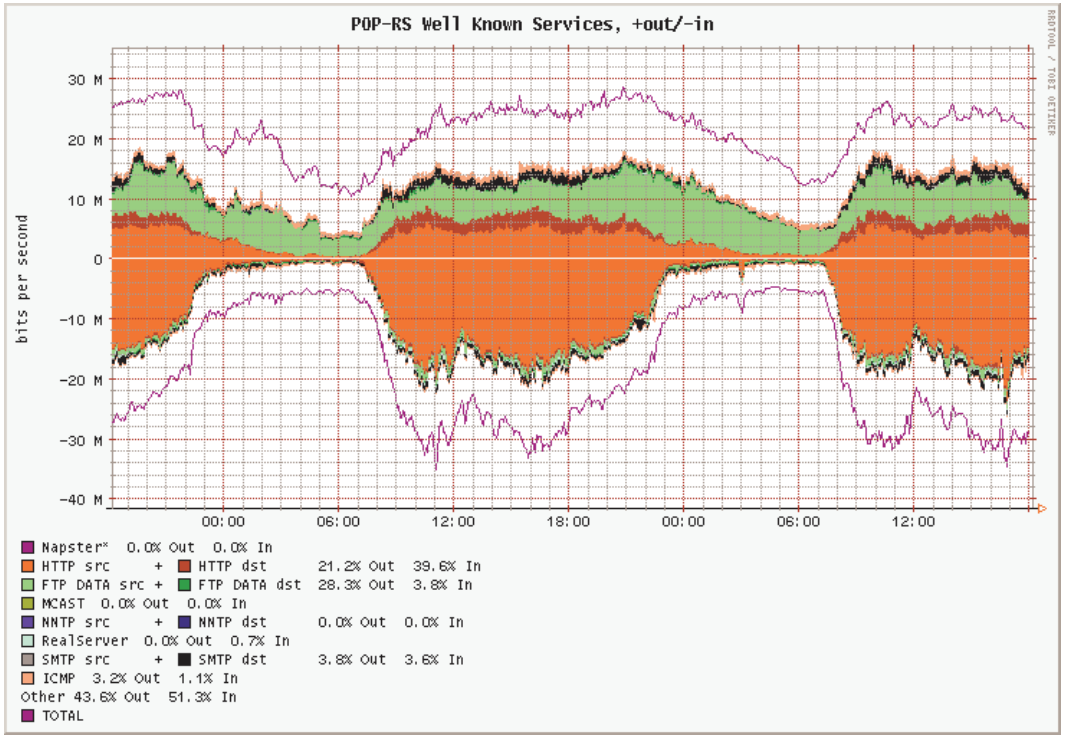
Top 20 143.54.0.0/16 hosts by **bytes out**
for five minute flow sample ending Fri Feb 21 20:27:32 2003

rank	src Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	143.54.28.105	37.0 k (0.5%)	2.1 M (54.1%)	103.5 (9.2%)	188.2 (14.2%)	473.3 m (1.1%)	713.3 m (0%)
#2	143.54.19.156	321.2 k (4.0%)	364.1 k (9.4%)	45.0 (4.0%)	51.0 (3.8%)	476.7 m (1.1%)	560.0 m (0%)
#3	143.54.47.240	10.3 (0.0%)	132.1 k (3.4%)	26.7 m (0.0%)	275.2 (20.8%)	26.7 m (0.1%)	93.8 (63%)
#4	143.54.1.3	7.2 k (0.1%)	126.6 k (3.3%)	11.7 (1.0%)	18.6 (1.4%)	700.0 m (1.6%)	866.7 m (1%)
#5	143.54.88.18	38.6 k (0.5%)	124.3 k (3.2%)	84.0 (7.5%)	49.0 (3.7%)	1.4 (3.1%)	1.4 (1%)

Nesse momento o primeiro da lista é um bom usuário de KazaA ☺

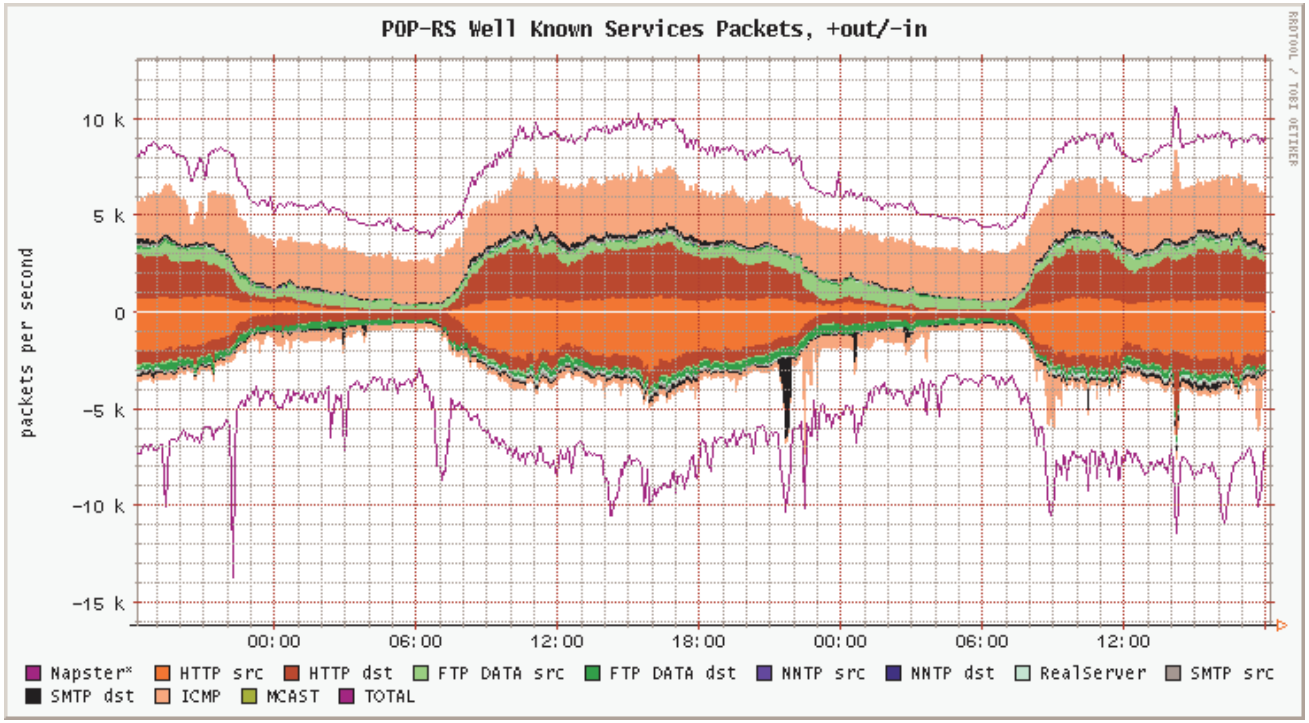
DOS e Netflow

Através do Netflow pode-se visualizar algo suspeito na rede...



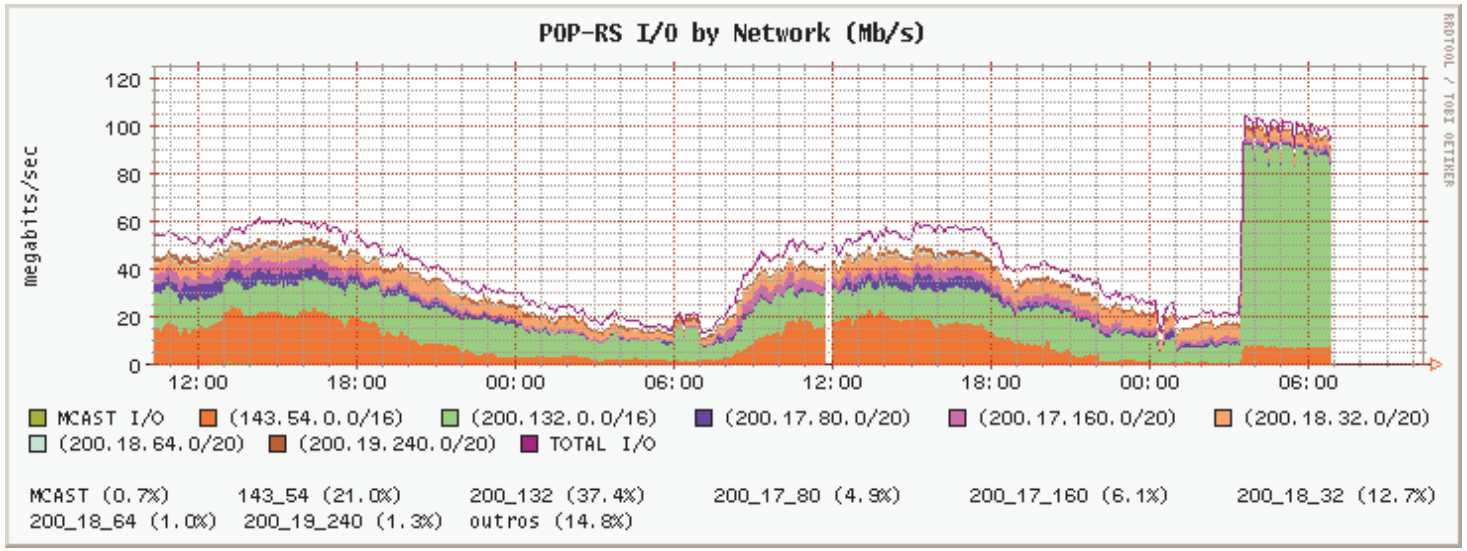
DOS e Netflow

...e detectar facilmente um *DOS* em andamento



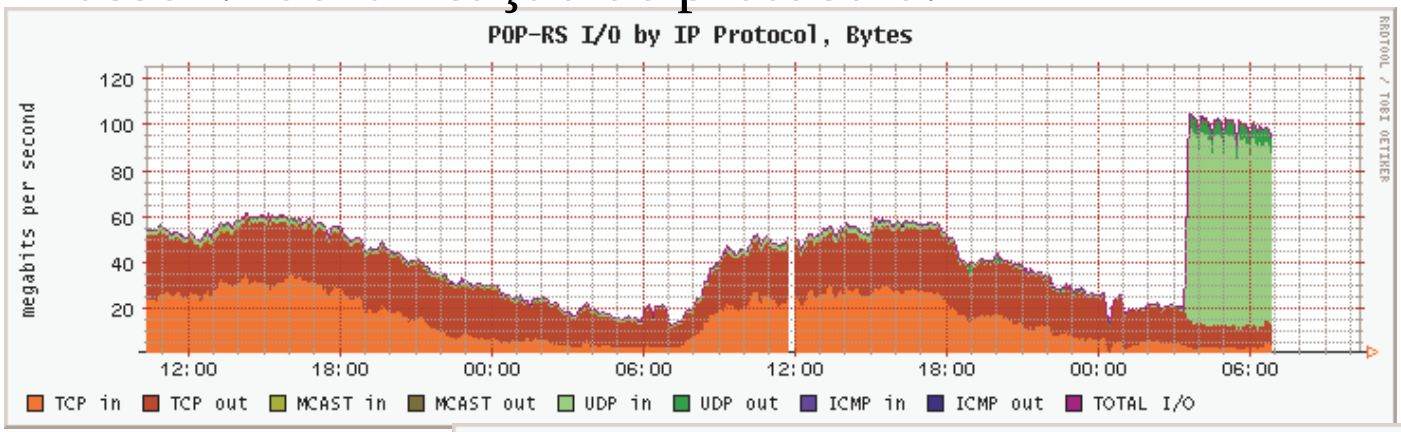
Ataque de worm´s

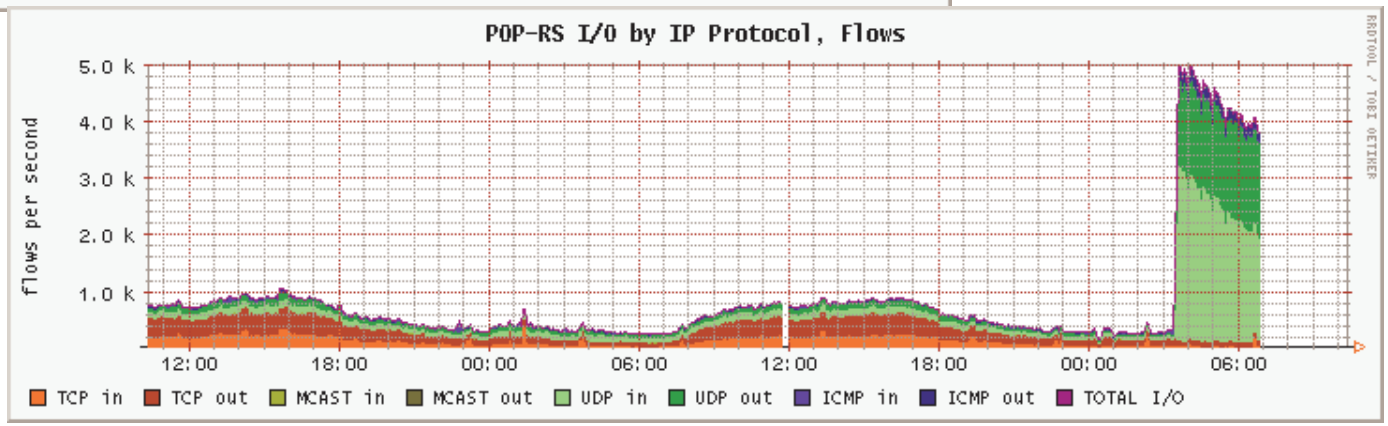
Passo1: Identificação do tráfego de cada bloco no backbone.



Ataque de worm´s

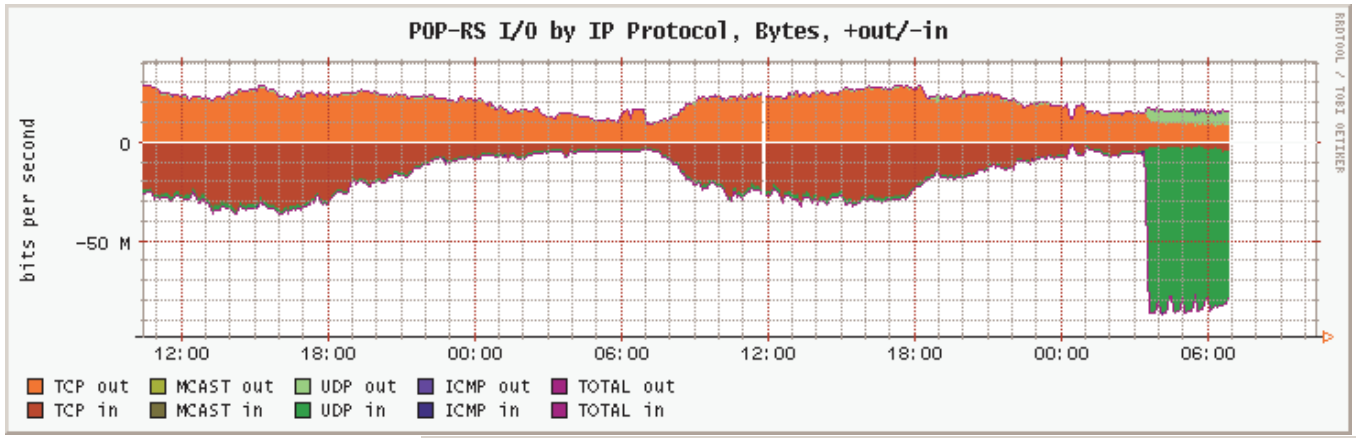
Passo2: Identificação de protocolo:

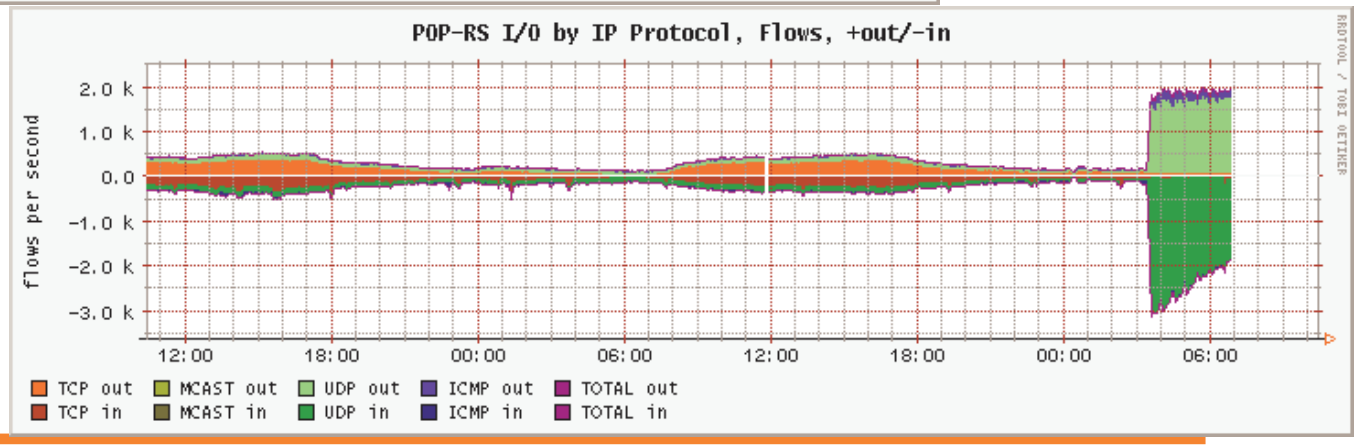




Ataque de worm´s

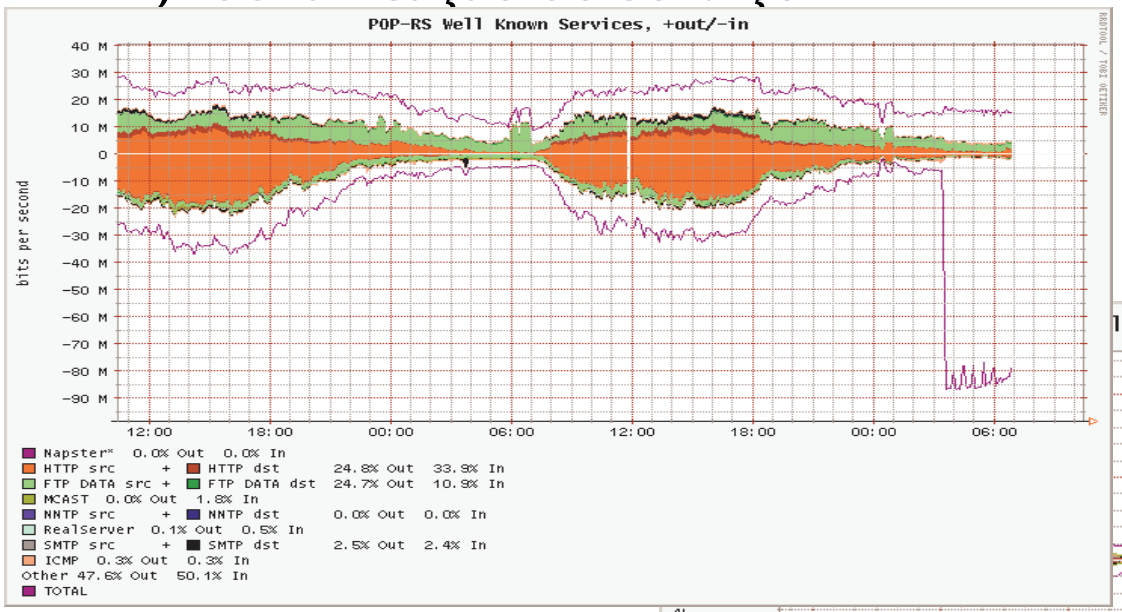
Passo3: Identificação do sentido do tráfego anormal:

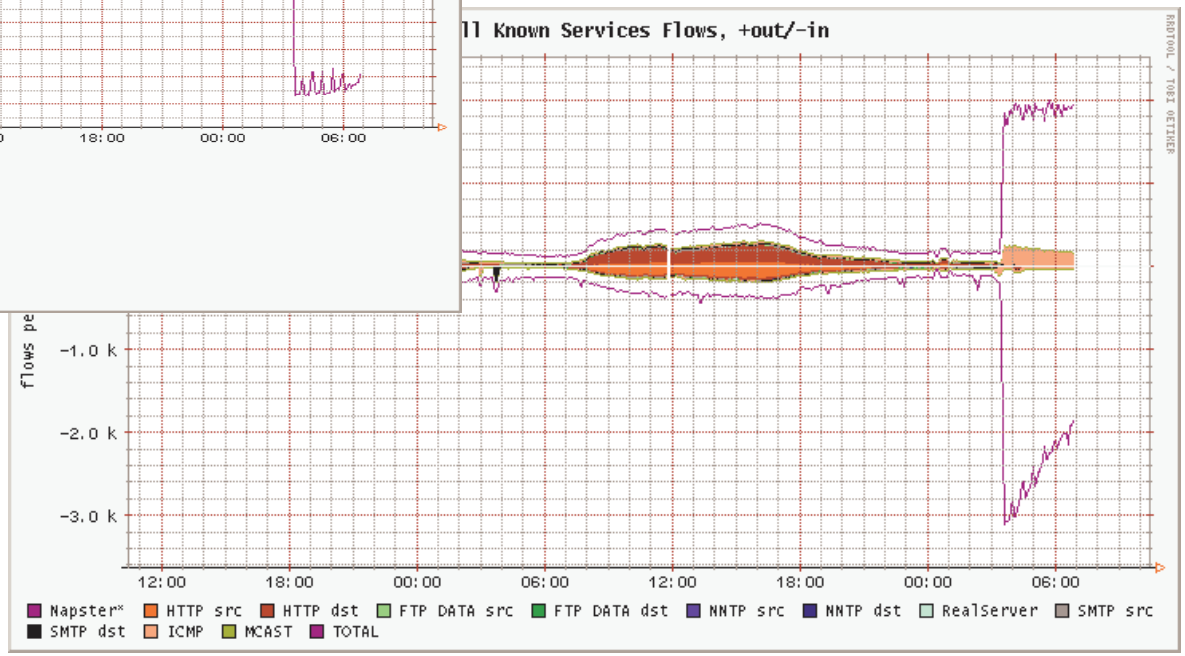




4) Identificação do serviço

Ataque de worm´s





Implementação no POP-RS

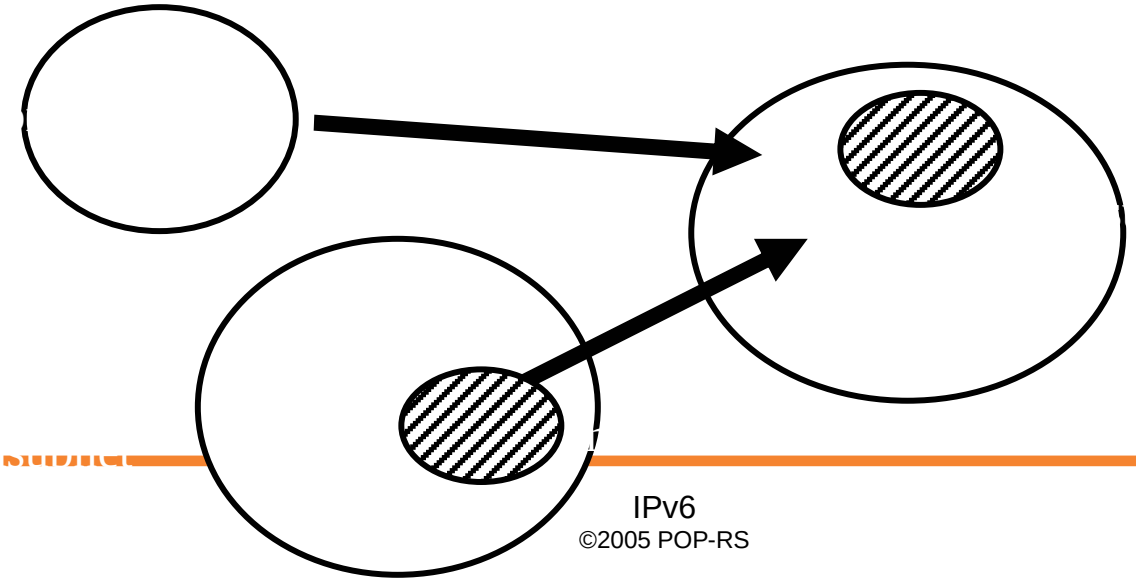
- Script em PERL
  - Gráficos são gerados dinamicamente (CGI)
  - Armazena dados em base de dados RRD
  - Bastante robusto
  - Baixa perfomance

Implementação no POP-RS

- Codificado sob ***CUFlow***

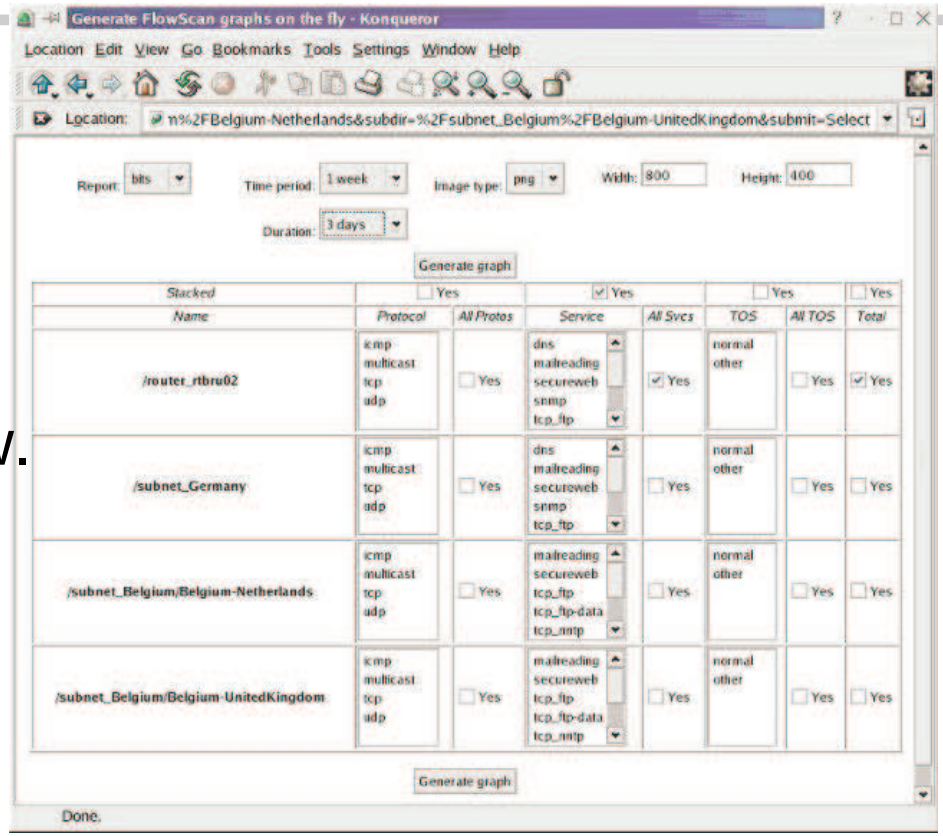
  \+ monitoramento protocolos/servicos por subrede +separar protocolos/servicos por roteador e subrede - código redundante
- Modulo independente
- URL: *http://users.telenet.be/jurgen.kobierczynski*

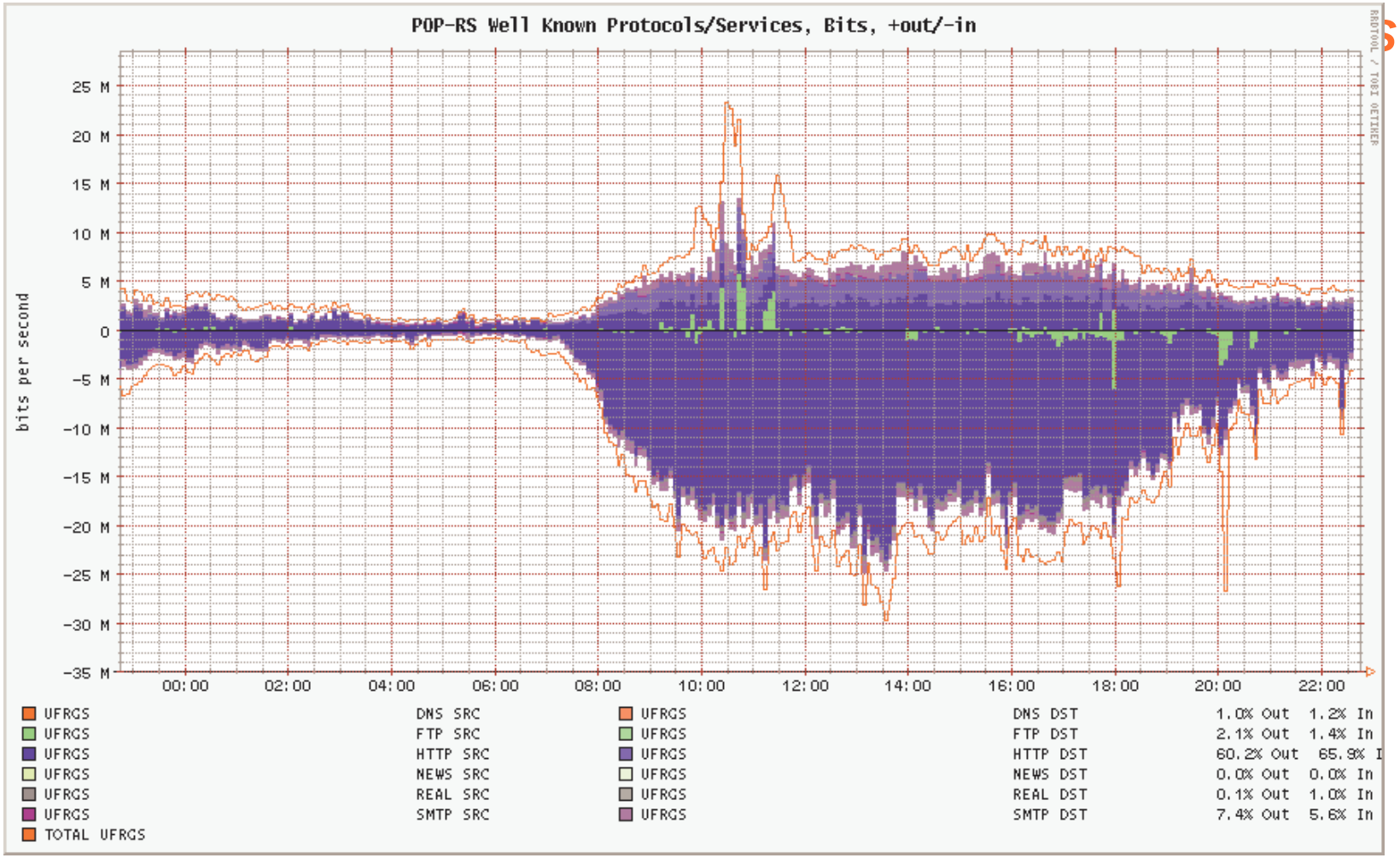
- Introduz o conceito de direções:
  - Selecionar Origem/Destino
  - Excluir Origem/Destino
    - Todo trafego que sai da minha universidade, vai para a rede da USP, que não seja oriundo do IP XXX, e não seja HTTP.



JKGrapher
CGI-script

- CGI-script para ler arquivos RRDTool criados pelo JKFlow.
- Baseado no CUGrapher




POP-RS Well Known Protocols/Services, Bits, +out/-in
bits per second
25 M
20 M
15 M
10 M
5 M
0
-5 M
-10 M
-15 M
-20 M
-25 M
-30 M
-35 M
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
UFRGS
UFRGS
UFRGS
UFRGS
UFRGS
UFRGS
TOTAL UFRGS
DNS SRC
FTP SRC
HTTP SRC
NEWS SRC
REAL SRC
SMTP SRC
UFRGS
UFRGS
UFRGS
UFRGS
UFRGS
UFRGS
DNS DST 1.0% Out 1.2% In
FTP DST 2.1% Out 1.4% In
HTTP DST 60.2% Out 65.9% I
NEWS DST 0.0% Out 0.0% In
REAL DST 0.1% Out 1.0% In
SMTP DST 7.4% Out 5.6% In

Relatório de Worms

- Worm beagle-w
  - Requisições a servidores infectados
  - Symantec
    - http://www.sarc.com/avcenter/venc/data/w32.beagle.w@mm.html

Computer Emergency Response Team - Rio Grande do Sul
Seguranca pro-ativa

Relatório do worm Beagle-W

Hosts possivelmente infectados pelo worm beagle

rank	IP	flows	octets	packets
1	X.X.X.X	27 (24.55%)	130,714 (51.82%)	1,735 (65.27%)
2	X.X.X.X	14 (12.73%)	58,888 (23.35%)	389 (14.64%)
3	X.X.X.X	14 (12.73%)	50,186 (19.90%)	374 (14.07%)
4	X.X.X.X	2 (1.82%)	6,339 (2.51%)	56 (2.11%)
5	X.X.X.X	13 (11.82%)	1,872 (0.74%)	39 (1.47%)
6	X.X.X.X	2 (1.82%)	720 (0.29%)	12 (0.45%)
7	X.X.X.X	1 (0.91%)	705 (0.28%)	5 (0.19%)
8	X.X.X.X	1 (0.91%)	469 (0.19%)	6 (0.23%)
9	X.X.X.X	7 (6.36%)	420 (0.17%)	7 (0.26%)
10	X.X.X.X	6 (5.45%)	360 (0.14%)	6 (0.23%)
11	X.X.X.X	6 (5.45%)	360 (0.14%)	6 (0.23%)
12	X.X.X.X	2 (1.82%)	288 (0.11%)	6 (0.23%)
13	X.X.X.X	4 (3.64%)	240 (0.10%)	4 (0.15%)
14	X.X.X.X	2 (1.82%)	208 (0.08%)	4 (0.15%)
15	X.X.X.X	2 (1.82%)	96 (0.04%)	2 (0.08%)
16	X.X.X.X	2 (1.82%)	88 (0.03%)	2 (0.08%)
17	X.X.X.X	1 (0.91%)	60 (0.02%)	1 (0.04%)
18	X.X.X.X	1 (0.91%)	60 (0.02%)	1 (0.04%)
19	X.X.X.X	1 (0.91%)	60 (0.02%)	1 (0.04%)
20	X.X.X.X	1 (0.91%)	52 (0.02%)	1 (0.04%)

Conclusões

- Possibilita uma boa visão da rede
- Possibilita um reação rápida
- Bastante robusto

Bibliografia

- Cisco Systems Inc. NetFlow Services and Applications – White Paper.http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm.
- Cflowd: Traffic FlowAnalysis Toolhttp://www.caida.org/tools/measurement/cflowd/
- Analysis of the Sapphire Worm - A joint effort of CAIDA, ICSI, Silicon Defense, UC Berkeley EECS and UC San Diego CSE. http://www.caida.org/analysis/security/sapphire/.
- Claise, B.; Cisco Systems NetFlow Services Export Version 9. http://www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt.
- FlowScan - Network Traffic Flow Visualization and Reporting Toolhttp://www.caida.org/tools/utilities/flowscan/index.xml
- Flow-tools Information. http://www.splintered.net/sw/flow-tools/[I2 2003] Internet 2 NetFlow Statistics. http://netflow.internet2.edu/.

Dúvidas, questionamentos, sugestões...

Contato no POP-RS

suporte@pop-rs.rnp.br

Contato:

ceron@tche.br

Obrigado!