PRÁTICA EM SEGURANÇA DE REDES: EXPERIÊNCIAS COM NETFLOW

Andrey Vedana Andreoli, Leandro Márcio Bertholdo e
Liane M. R. Tarouco

CERT-RS / POP-RS / UFRGS
Rua Ramiro Barcelos, 2574 - Porto Alegre – RS

{andrey, berthold, liane}@penta.ufrgs.br

Resumo

Como as redes se tornaram grandes e heterogêneas, os administradores necessitam de ferramentas eficientes para monitorar as atividades da rede a aplicar uma segurança global em seus backbones. Em ambientes abertos, como redes acadêmicas e de pesquisa, a restrição de acesso do usuário a aplicações nem sempre é uma opção, dessa forma o controle de uso dos recursos é imprescindível.

Ferramentas que sempre foram utilizadas para análise de rede como: TCPDump, Trafshow, LANExplorer, Ethereal e outras, já não conseguem manipular satisfatoriamente grandes quantidades de tráfego a um custo viável para essas instituições.

Nessa apresentação descrevemos um conjuntos de ferramentas que analisam fluxos de dados (NetFlow) gerados por vários nodos da rede. Essas ferramentas são usadas a alguns anos pelo POP-RS/RNP e pelo CERT-RS para diagnosticar, contabilizar e tratar os incidendes detectados a partir do controle do próprio backbone. Hoje, o tráfego agregado deste supera a marca dos 70 Mbps.Essa abordagem nos permitiu rapidamente diagnosticar e controlar vários Denial of Services realizados contra e/ou utilizando instituições conectadas ao Ponto de Presença da RNP no Rio Grande do Sul.

Sumário

- O que é *"NetFlow"*?
- Ferramentas utilizadas no CERT-RS
  - Utilizando a Interface dos equipamentos
  - Cflowd
  - ARTS
  - Flowscan
  - Flow-Tools
  - Ntop
- Estudo de Caso: O Verme Slammer
- Netflow na I2
- Conclusões e Direções Futuras

Definição do termo “flow” e características gerais

- Registro Netflow (flow): Sequência unidirecional de pacotes entre dois pontos de comunicação. Uma vez identificado o fluxo, são armazenadas as seguintes informações:
  - Conjunto IP/porta origem
  - Conjunto IP/porta destino
  - Tipo de protocolo
  - TOS (Type of Service)
  - Interface de entrada do fluxo
  - Hora inicial e final do fluxo
  - Nùmero de pacotes e octetos
  - Sistema autônomo origem e destino

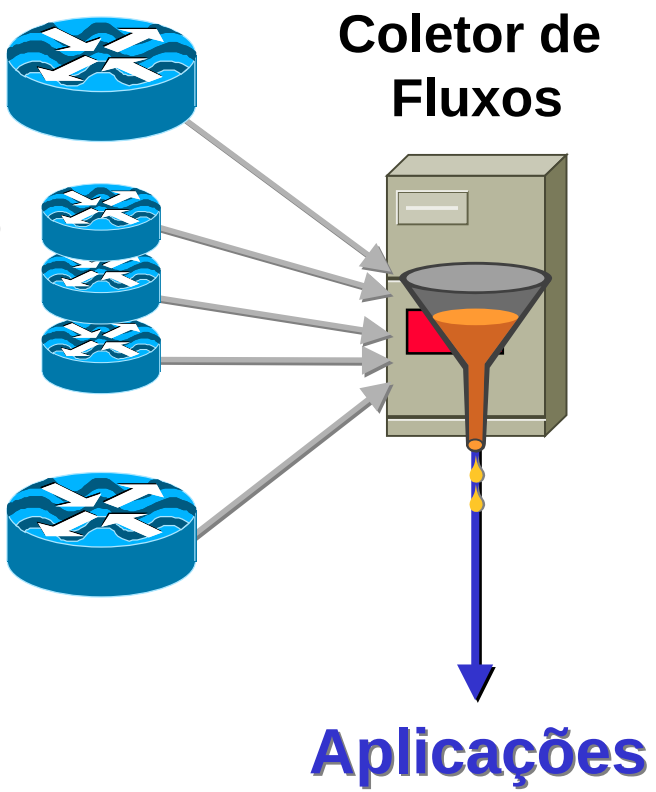
Condições para criação de flows

Existem condições específicas para o início ou final de um fluxo (flow). São elas:

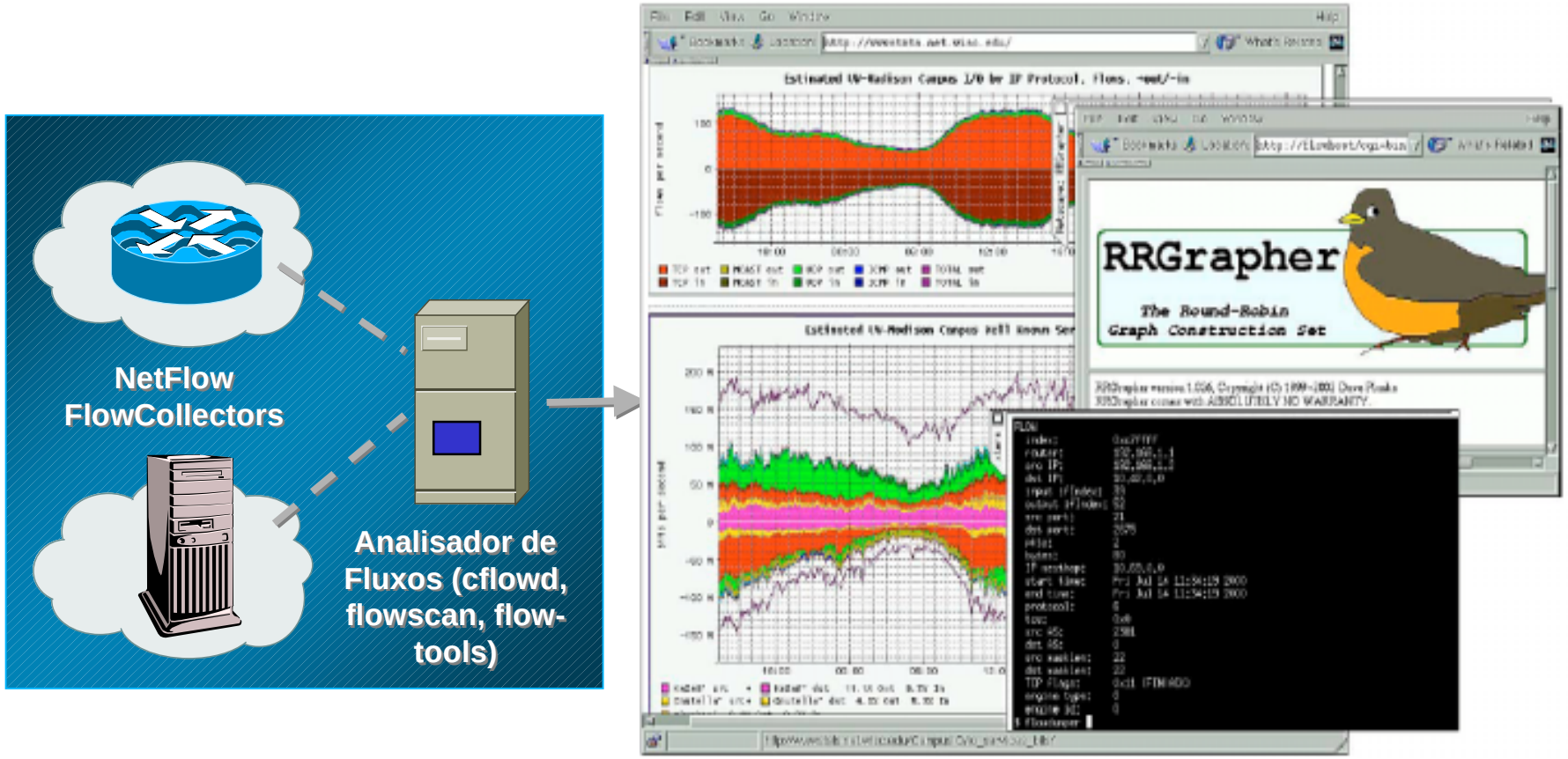
- Em conexões TCP, quando a conexão for encerrada (depois de um RST ou FIN);
- Quando não ocorrer tráfego durante 15 segundos;
- Caso o tempo exceder os 30 minutos a partir do início do fluxo;
- Quando a tabela de fluxos estiver cheia;

NETFLOW

- Conjunto de ferramentas para monitoração de tráfego e exportação de modelos de dados.
- Surgiu em 1996 em implementação da Cisco.
- Encontrada atualmente em equipamentos Cisco, Juniper, Extreme, entre outros.
- O IETF redigiu draft-bclaise-netflow-9-00.txt (Jun/2002) para o Netflow v9



Fluxo de Informações no Netflow



Conjunto de Ferramentas Utilizadas para extrair informações sobre os fluxos em andamento ou armazenados

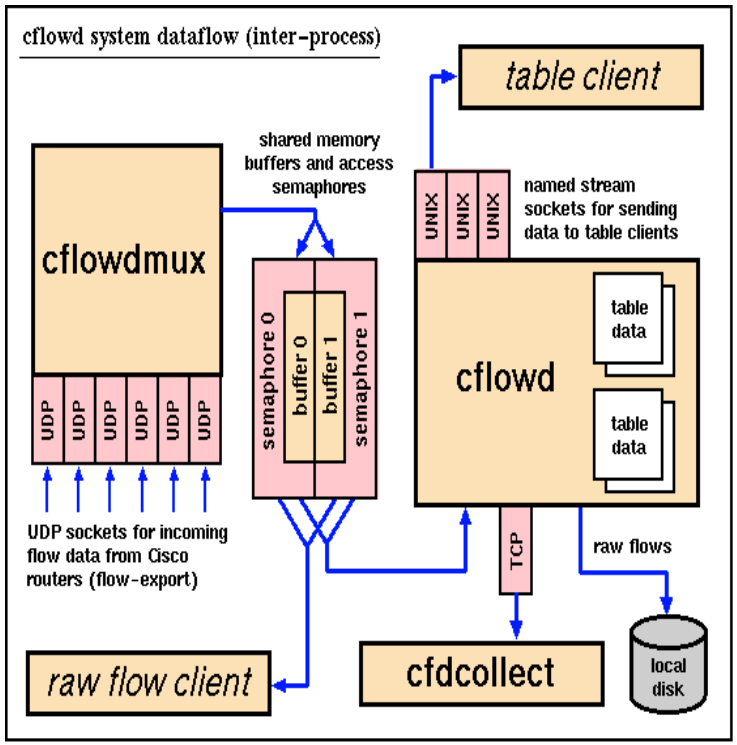
Interface do Equipamento

```
rs-bb3>sh ip cache flow
IP packet size distribution (8670M total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .001 .453 .058 .016 .010 .006 .006 .004 .005 .004 .003 .004 .004 .003 .003

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .003 .002 .064 .024 .319 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes  82 active, 65454 inactive, 4120535 added
   89798660 ager polls, 0 flow alloc failures  Active flows timeout in 1 minutes
   Inactive flows timeout in 15 seconds  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)------
   --          Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /FlowTCP-
   Telnet       834600      0.7        16   166     12.3       9.0      16.2TCP-
   FTP         5017218      4.4        10    86     46.1       4.4      15.7TCP-
   FTPD        2026874      1.8       278   992    504.1      45.1       2.7TCP-
   WWW       218687228    195.5        14   506   2791.2       5.9       9.3TCP-
   SMTP       27937130     24.9        10   385    268.9       6.1      11.4TCP-
   other     115224269    103.0        31   671   3253.9      12.9      12.0UDP-
   DNS        46205254     41.3         3    76    161.5       4.3      17.2UDP-
   NTP         2290487      2.0         1    75      2.5       0.2      17.3UDP-
   TFTP            794      0.0         3   212      0.0       2.2      16.3UDP-
   Frag          40824      0.0       154   734      5.6      49.8       4.7UDP-
   other     120392993    107.6         4   176    508.3       1.9      17.4ICMP
             19163422     17.1         5   101     93.2       4.0      17.1IGMP
                13612      0.0         1    28      0.0       0.0      15.5IPINIP
```

Cflowd

- Permite análise e armazenamento dos fluxos gerados pelo cisco netflow
- Possui quatro módulos
  - Cflowdmux: recebe os fluxos de dados e permite o compartilhamento com outras aplicações
  - Cflowd: recebe os dados coletados e os tabula (matriz de ASs, de redes, de portas, de interfaces e tabela de protocolos)
  - Cfdcollect: arquiva os dados coletados em uma base de dados.



Cflowd

- O quarto módulo é formado por utilitários
  - **Flowdump:** mesmo tratamento de ERs do tcpdump

```
flowdump -e '(protocol == 6) && (dstas == 4230) && \
         ((tcpflags & 0x02) == 0x02))' 200.132.0.17.flows.1
```

  - **Cfdnets:** mostra uma matriz de tráfego por redes

```
 source network         dest network          pkts/sec          bits/sec
  -----------------  -----------------  --------------  --------------
143.54.0.0/16         18.0.0.0/ 8                0              113
143.54.0.0/16         35.0.0.0/ 8                0                3
143.54.0.0/16        193.0.0.0/21                0               71
143.54.0.0/16        128.2.0.0/16                0                7
143.54.0.0/16        152.2.0.0/16                0               30
```

Cflowd

– **cfdportmatrix:** matriz de portas em uso

srcPort	dstPort	packets	bytes	pkts/sec	bits/sec
0	25	57	2280	1	337
1024	53	260	17519	4	2595
1024	80	6	939	0	139
1280	80	31	7786	0	1153
1280	3978	2174	3253128	40	481944

– **cfdprotos:** tabela de protocolos utilizados

protocol	packets	bytes	pkts/sec	bits/sec
icmp	395	55756	16	18585
tcp	114897	72523318	4787	24174439
udp	4953	612455	206	204151
ipv6	2	184	0	15

ARTS

- ARTS é um formato binário para armazenar informações de rede. São armazenados:

forward IP path	interface matrix
AS matrix	nexthop table
net matrix	TOS table
port matrix	RTT time series

- ARTS também possui vários utilitários para pesquisa na base de dados:
  - artsases, artsnets, artsprotos, artsports, artstos e outros.

Flowscan, RRDTool e RRGrapher.cgi

- O **Flowscan** é utilizado para armazenar os dados coletados pelo CFLOWD e aqueles armazenados na base ARTS para o formato RRD (Round Robin Database)

- O **RRDTool** permite a geração de gráficos pré-definidos.

- **RRGrapher.cgi** é um aplicativo em perl que permite definir através de uma interface web qual gráfico será traçado. Esse é traçado somente no momento da solicitação – o que diminui os gastos com CPU.

Flowscan

Top 20 origin ASNs by bytes **in**
for five minute flow sample ending Fri Feb 21 20:27:32 2003

rank	origin-AS	bits/sec in	% of total in	bits/sec out	% of total out
#1	unidentified	7.2 M	34.9%	10.7 M	36.9%
#2	LACNIC-1251 (1251)	6.6 M	32.1%	170.6 k	0.6%
#3	LACNIC-4230 (4230)	1.1 M	5.1%	996.9 k	3.4%
#4	SASK-RESEARCH-NETWORK (26300)	963.0 k	4.7%	15.8 k	0.1%
#5	RIT-ASN (4385)	648.7 k	3.2%	17.6 k	0.1%

Top 20 path ASNs by bytes **in**
for five minute flow sample ending Fri Feb 21 20:27:32 2003

rank	path-AS	bits/sec in	% of total in	bits/sec out	% of total out
#1	LACNIC-1251 (1251)	6.6 M	32.1%	170.6 k	0.6%
#2	ABILENE (11537)	3.4 M	16.5%	438.5 k	1.5%
#3	LACNIC-4230 (4230)	1.6 M	7.6%	1.7 M	5.8%
#4	NYSERNET3-AS (3754)	1.0 M	5.0%	23.5 k	0.1%
#5	CANARIE-NTN (6509)	963.3 k	4.7%	23.1 k	0.1%

Flowscan

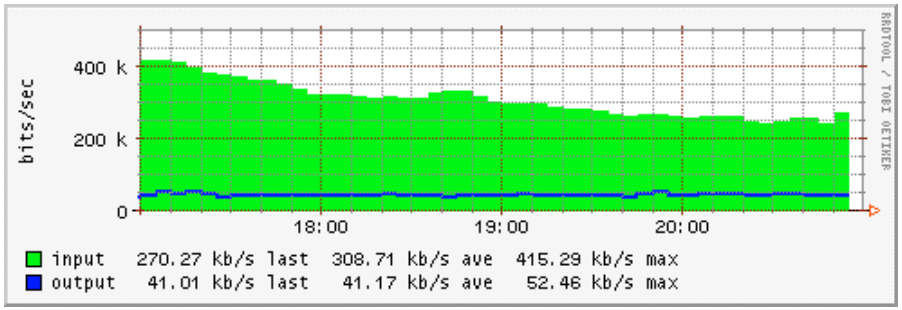
Top 20 143.54.0.0/16 hosts by **bytes out**
for five minute flow sample ending Fri Feb 21 20:27:32 2003

rank	src Address	bits/sec in	bits/sec out	pkts/sec in	pkts/sec out	flows/sec in	flows/sec out
#1	A.A.A.A	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	B.B.B.B	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	C.C.C.C	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	D.D.D.D	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	E.E.E.E	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 ☺

Tráfego gerado pelo Netflow

- Um dos grandes problemas é a quantidade de dados. No POP-RS ~1Gb/dia são gerados pelo netflow e armazenados.



Flow-tools

Conjunto de ferramentas utilizadas para o recebimento e armazenamento de fluxos gerados pelo Netflow. Possui diversas ferramentas utilizadas para a análise dos fluxos, listados a seguir:

- Flow-Expire
  - Remove fluxos antigos, baseado na utilização de disco.
  - Utilizado também em ambientes onde o armazenamento é feito em ambiente distribuído.

- Flow-print

Flow-tools

  - Exibe arquivos de flows com dados formatados.

```
% flow-print < ft-v05.2002-01-21.093345-0500 | head -15
srcIP            dstIP            prot  srcPort  dstPort  octets packets
131.238.205.199  194.210.13.1     6     6346     40355    221          5
192.5.110.20     128.195.186.5    17    57040    33468    40           1
128.146.1.7      194.85.127.69    17    53       53       64           1
193.170.62.114   132.235.156.242  6     1453     1214     192          4
134.243.5.160    192.129.25.10    6     80       3360     654          7
132.235.156.242  193.170.62.114   6     1214     1453     160          4
130.206.43.51    130.101.99.107   6     3226     80       96           2
206.244.141.3    128.163.62.17    6     35593    80       739          10
206.244.141.3    128.163.62.17    6     35594    80       577          6
212.33.84.160    132.235.152.47   6     1447     1214     192          4
```

- Flow-Filter

Flow-tools

  - Filtra flows baseadas em porta, protocolo, AS number, IP, ToS, TCP bits e tags.

```
% flow-cat . | flow-filter -P119 | flow-print | head -10

srcIP            dstIP            prot  srcPort  dstPort  octets      packets
155.52.46.50     164.107.115.4    6     33225    119      114         2
128.223.220.29   129.137.4.135    6     52745    119      1438382     1022
155.52.46.50     164.107.115.4    6     33225    119      374         6
164.107.115.4    192.58.107.160   6     60141    119      5147961     8876
128.223.220.29   129.137.4.135    6     52745    119      1356325     965
128.223.220.29   129.137.4.135    6     52714    119      561016      398
130.207.244.18   129.22.8.64      6     36033    119      30194       121
155.52.46.50     164.107.115.4    6     33225    119      130         2
198.108.1.146    129.137.4.135    6     17800    119      210720652   216072
```

- Flow-dscan
  - Detecção de DoS e scans.
  - Detecta hosts que possuem muitas flows para outros hosts.
  - Detecta hosts que esteja utilizando grande número de portas TCP/UDP.
  - Indicado principalmente para redes menores ou com filtros que não limitem demasiadamente o tráfego.

Flow-tools

- Flow-stat
  - Gera relatório a partir de arquivos de flows.
  - Facilidade na importação de dados para programas de geração de gráficos, como o gnuplot.
  - Inclui em seus relatórios informações como IP, pares de IPs, portas, número de pacote, número de bytes, next hop, AS, ToS bits, router originador e tags.

- Flow-stat-summary

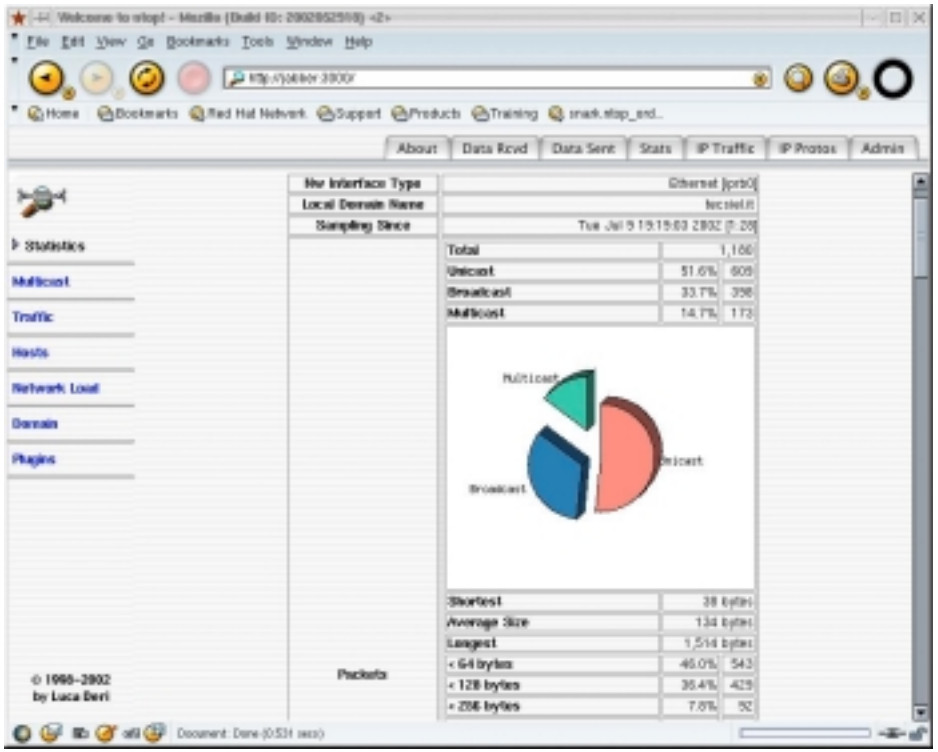
Flow-tools

  - Gera relatórios contendo totais e médias de flows, octetos, pacotes, duração das flows, médida de pacotes das flows, entre outras informações.

Total Flows : 24236730
Total Octets : 71266806610
Total Packets : 109298006
Total Time (1/1000 secs) (flows): 289031186084
Duration of data (realtime) : 86400
Duration of data (1/1000 secs) : 88352112
Average flow time (1/1000 secs) : 11925.0000
Average packet size (octets) : 652.0000
Average flow size (octets) : 2940.0000
Average packets per flow : 4.0000
Average flows / second (flow) : 274.3201
Average flows / second (real) : 280.5177
Average Kbits / second (flow) : 6452.9880
Average Kbits / second (real) : 6598.7781

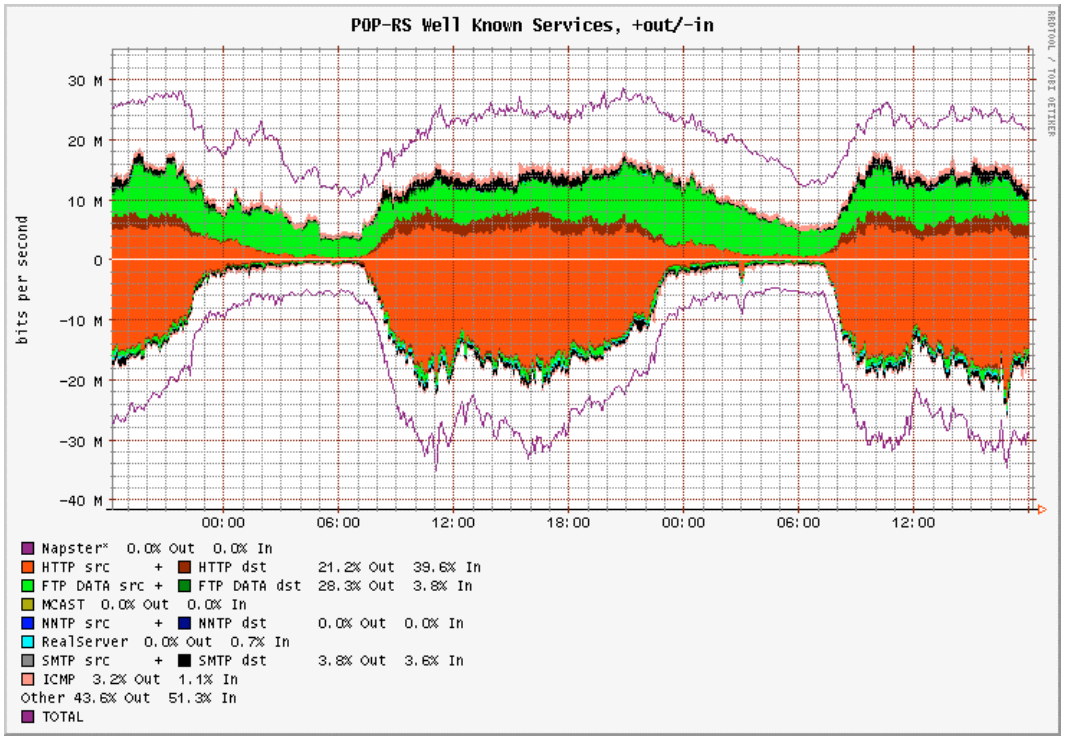
Ntop

- A versão 2 de NTOP permite exportar dados coletados por hosts situados em diferentes sub-redes no formato netflow v5 (ex. firewall, servidor web, etc.)



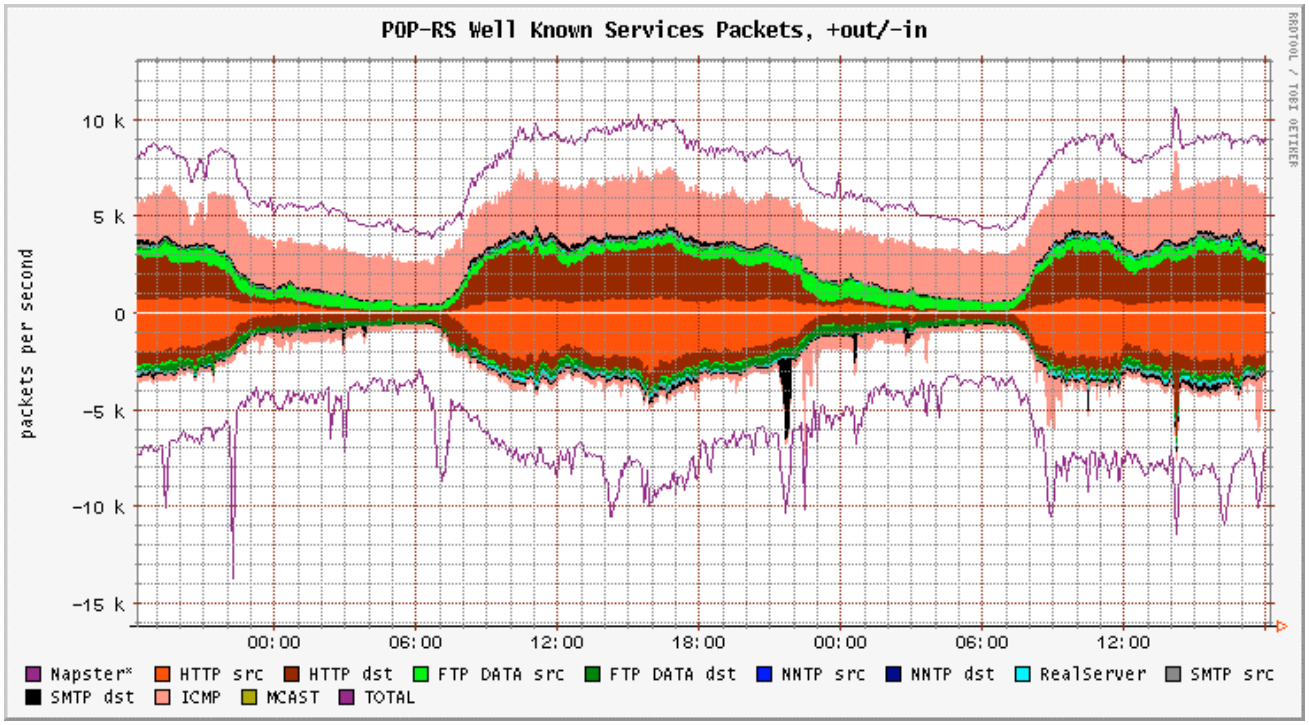
DOS e Netflow

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



DOS e Netflow

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



Estudo de Caso: SLAMMER (sapphire)...

Slammer worm (Sapphire worm)

25

3:30 ( ),

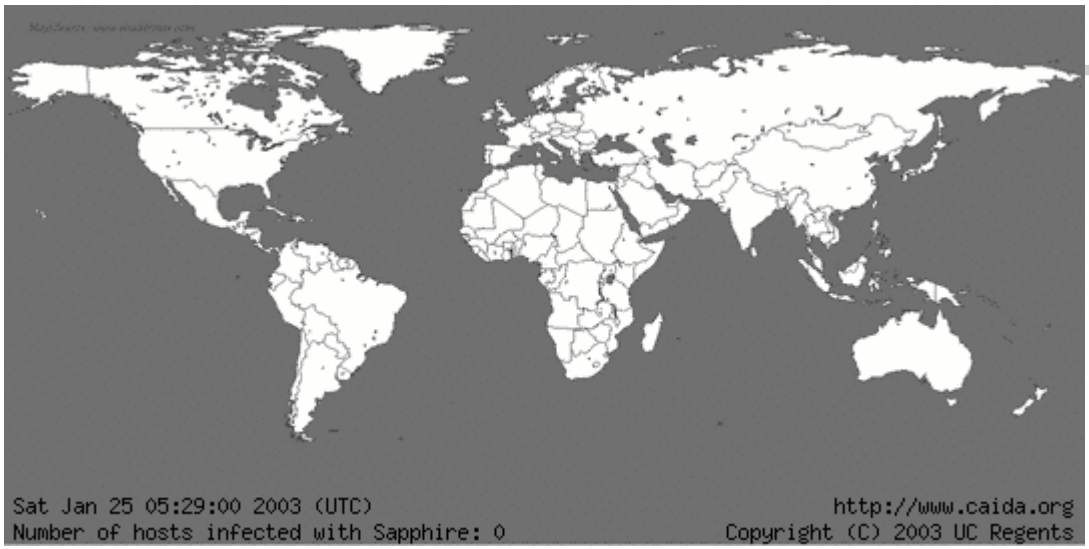
,

1434 .

Alguns relatos:

“This worm required roughly 10 minutes tospread worldwide making it by far the fastest worm to date” NANOG list.

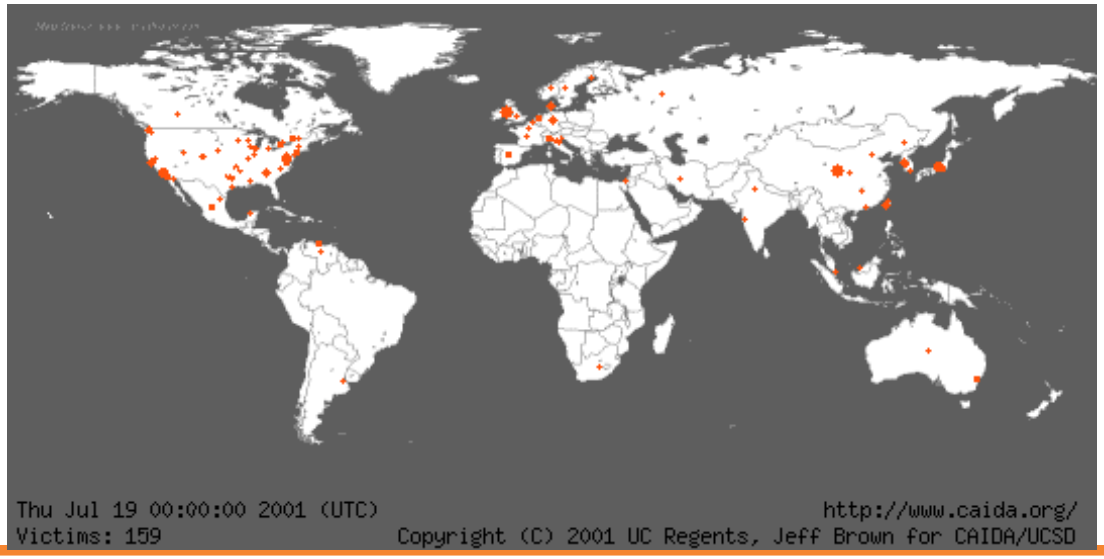
"SEATTLE (Reuters) - Bank of America Corp. said on Saturday that customers at a majority of its 13,000 automatic teller machines were unable to process customer transactions after a malicious computer worm nearly froze Internet traffic worldwide."



W32.Slammer

25/jan/2003
30min ~74mil hosts

Vs.



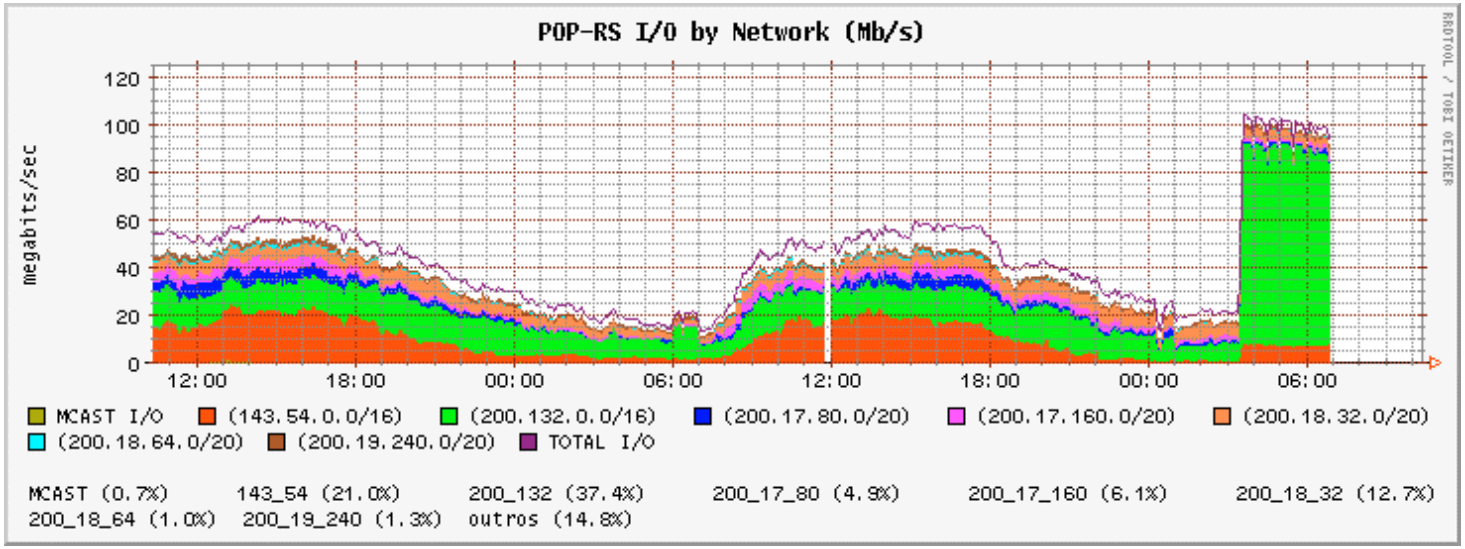
CodeRed v2

19/jul/2001
24h ~350mil hosts

fonte: www.caida.org

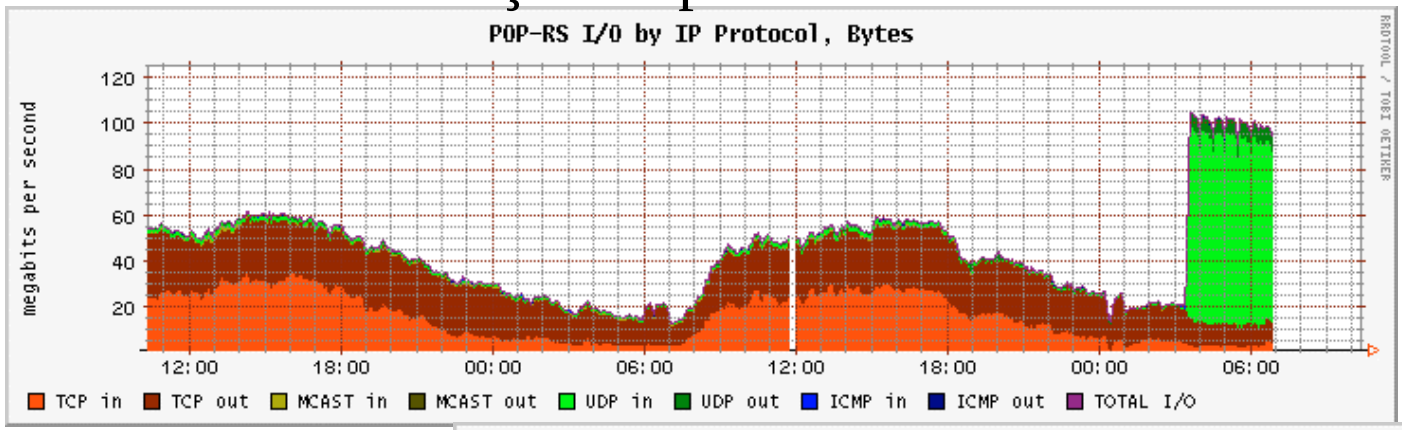
Slammer worm (Sapphire worm)

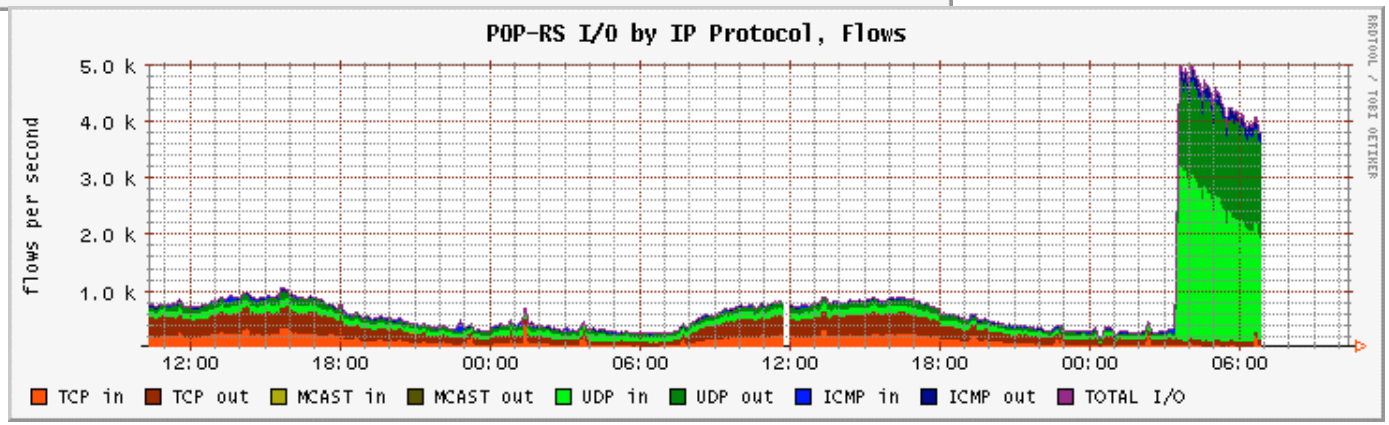
Passo1: Identificação do tráfego de cada bloco no backbone.



Slammer worm (Sapphire worm)

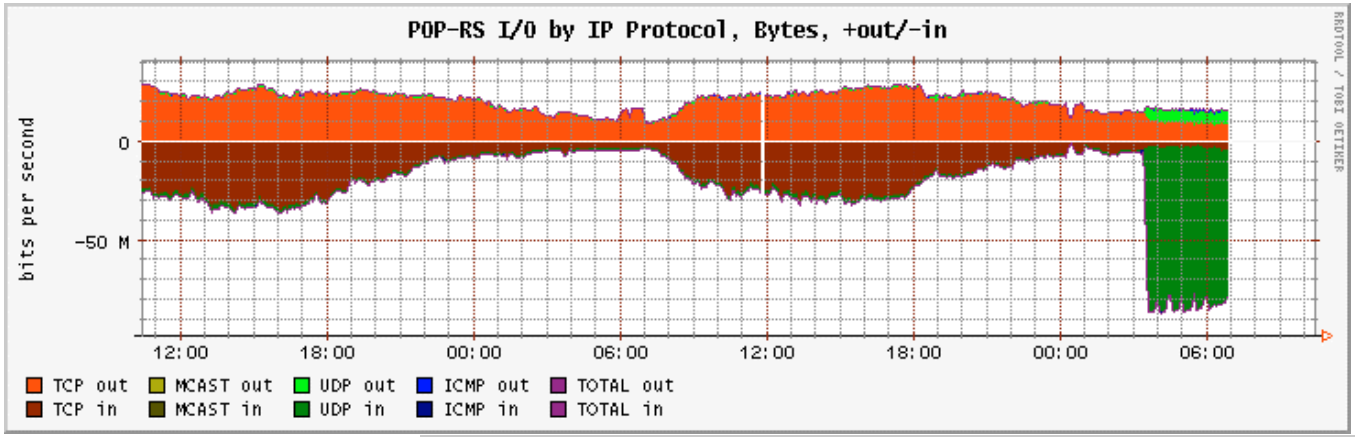
Passo2: Identificação de protocolo:

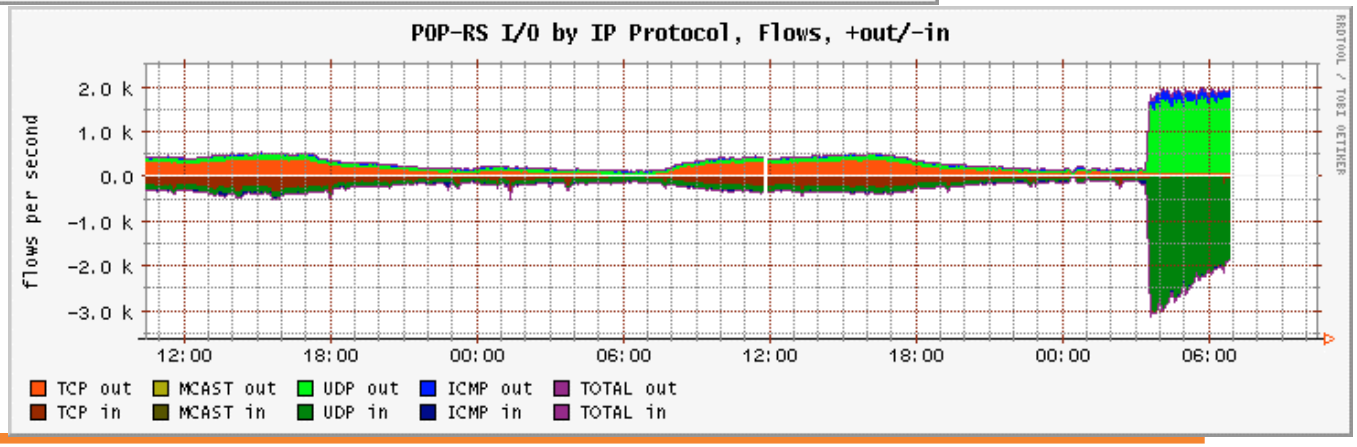




Slammer worm (Sapphire worm)

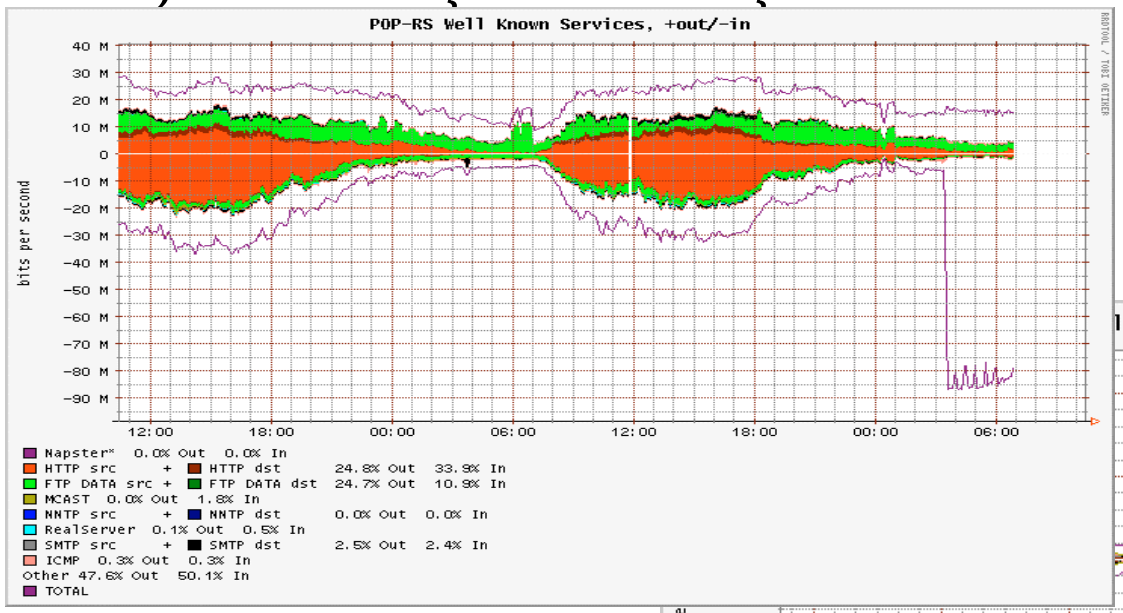
Passo3: Identificação do sentido do tráfego anormal:

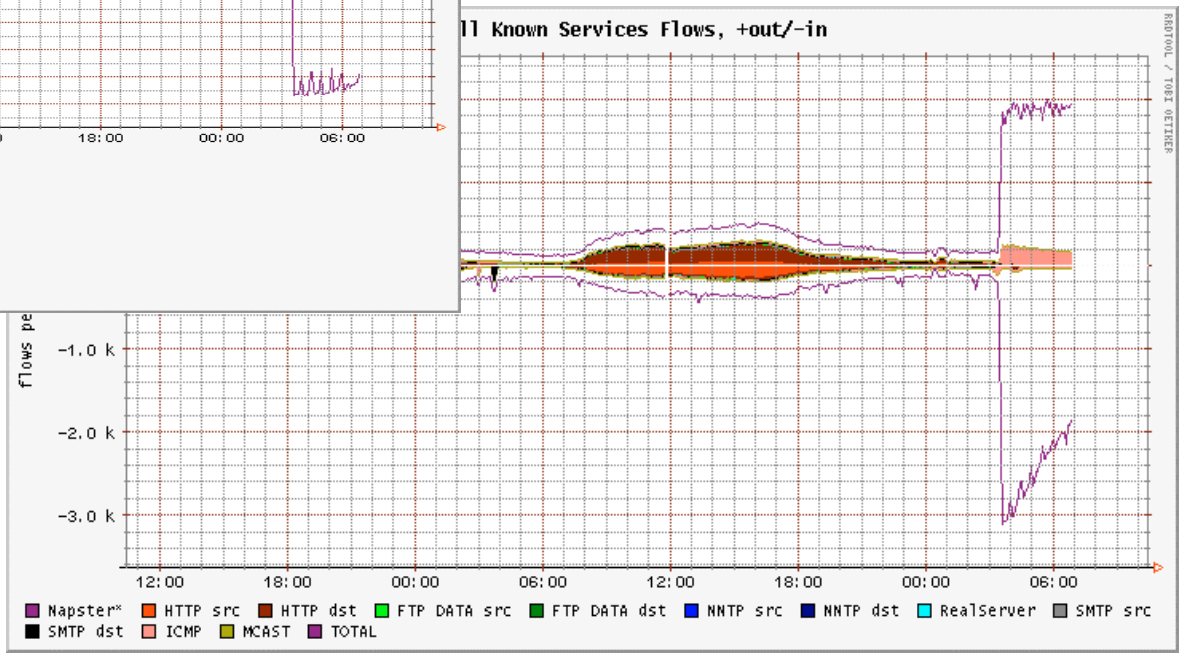




4) Identificação do serviço

Slammer worm





Slammer worm

5) Identificação na lista top-10 dos hosts que estavam gerando o tráfego e a porta utilizada

6) Filtragem no roteador de borda e normalização do tráfego.

```
access-list 199 deny   udp any eq 1434 any
access-list 199 deny   udp any any eq 1434
access-list 199 deny   udp any eq 1433 any
access-list 199 deny   udp any any eq 1433
access-list 199 deny   ip host A.A.A.A any
access-list 199 deny   ip host B.B.B.B any
access-list 199 deny   ip any host A.A.A.A
access-list 199 deny   ip any host B.B.B.B
access-list 199 permit ip any any
```

Netflow na Internet 2

- Dados do Netflow na I2 podem ser acessados em

http://netflow.internet2.edu/

Esse é uma prova da capacidade de escalabilidade do Netflow.

Requisitos de software e hardware

- No POP-RS esta sendo utilizado um Pentium IV 1500Mhz com 256Mb de RAM rodando FreeBSD. 30Gb de disco estão destinados ao Netflow, o que nos permite manter aproximadamente um mês de estatísticas
- Neste momento somente um router (Cisco 7507) esta gerando fluxo para ele.
- Durante o ataque (Slammer), o excesso de tráfego (>100Mbps) tornou insuficiente o hardware para o tamanho do fluxo gerado.

Conclusões e próximos passos

- Recurso importante para o CERT-RS e instituições da Rede Tchê não somente na área de engenharia, mas também na área de segurança.
  - Fornece informações detalhadas sobre o tráfego;
  - Permite medições e detecção de anormalidades de tráfego;
  - Detecção e traceback de ataques;
- Implementação de scripts para verificação de comportamentos anormais, reportando ao suporte do NOC;
- Documentação da experiência adquirida com Netflow será utilizada para criação de um módulo adicional ao curso de Segurança em Redes de Computadores promovido pelo GTRH.

Referências

[CIS 2002] Cisco Systems Inc. **NetFlow Services and Applications – White Paper**. http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm.

[CFL 2003] **Cflowd: Traffic Flow Analysis Tool** http://www.caida.org/tools/measurement/cflowd/

[CAI 2003] **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/.

[CLA 2002] Claise, B.; **Cisco Systems NetFlow Services Export Version 9.** http://www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt.

[FLO 2003] **FlowScan - Network Traffic Flow Visualization and Reporting Tool** http://www.caida.org/tools/utilities/flowscan/index.xml

[FLT 2003] **Flow-tools Information**. http://www.splintered.net/sw/flow-tools/

[I2 2003] **Internet 2 NetFlow Statistics**. http://netflow.internet2.edu/.

[SHA 2001] Shalunov, Stanislav; Teitelbaum, Benjamin. **Bulk TCP Use an Performance on Internet2.** http://abilene.internet2.edu/tcp/i2-tcp.pdf.

Contatos, dúvidas, sugestões, críticas, opiniões, ideias??