

ISPの中の運用と オープンソース 【実践編】

2010年10月23日 OSC新潟

高嶋隆一

自己紹介

□ 高嶋隆一

➤ ここ数年

- ✓ とあるIT企業でネットワーク・サーバの設計・構築・運用を担当

➤ もっと前

- ✓ とあるISPで設計・構築・運用を担当

□ ごめんなさい、**元**ISPです。

目次

- ISPのヒトが見たいモノ
- ツールの紹介
- 実用上の諸注意

注意事項

- 便宜上、NetFlow, sFlow等のFlow解析技術を“xFlow”
とひとまとめに呼んでいます。
- が、必ずしも一般的な呼称ではなく、
実装としてはそれぞれ異なる技術
です。

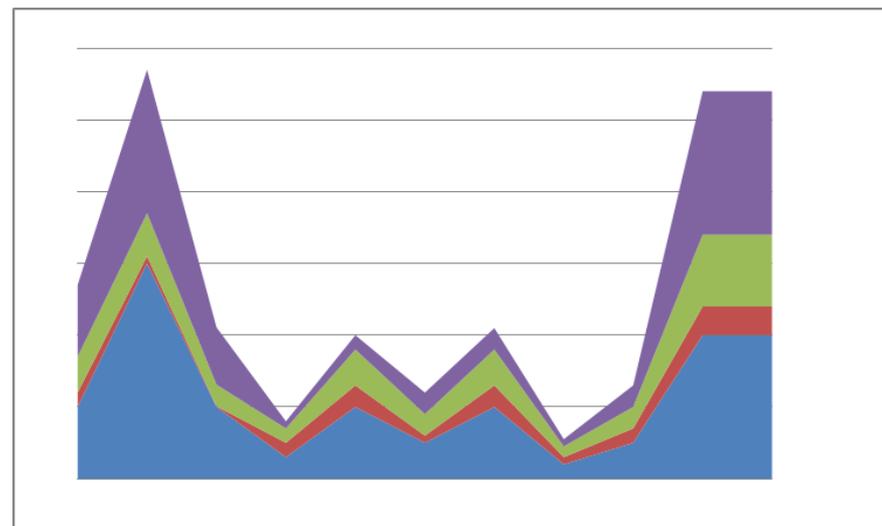
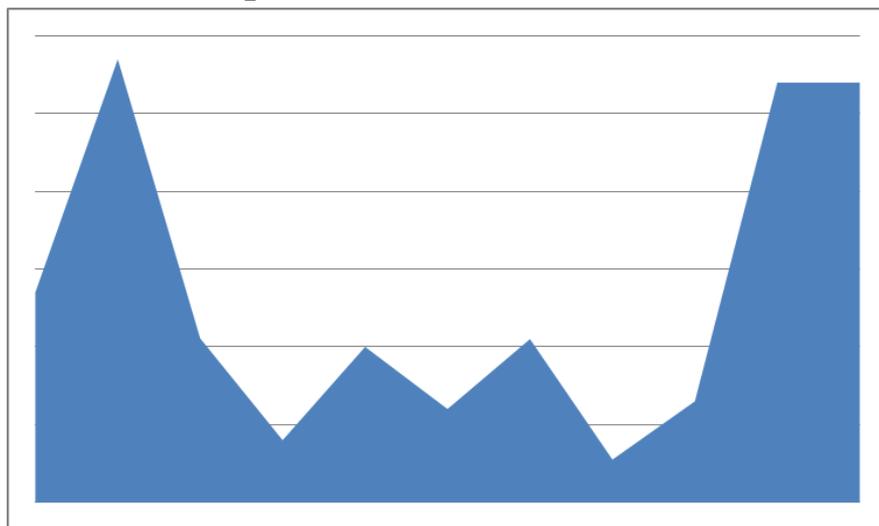
ISPのヒトがみたいもの

□それは「内訳」

- 「どんな」トラフィックが
「どこから」
「どこあて」に
きているかみたい!

ISPのヒトがみたいもの

□ イメージ



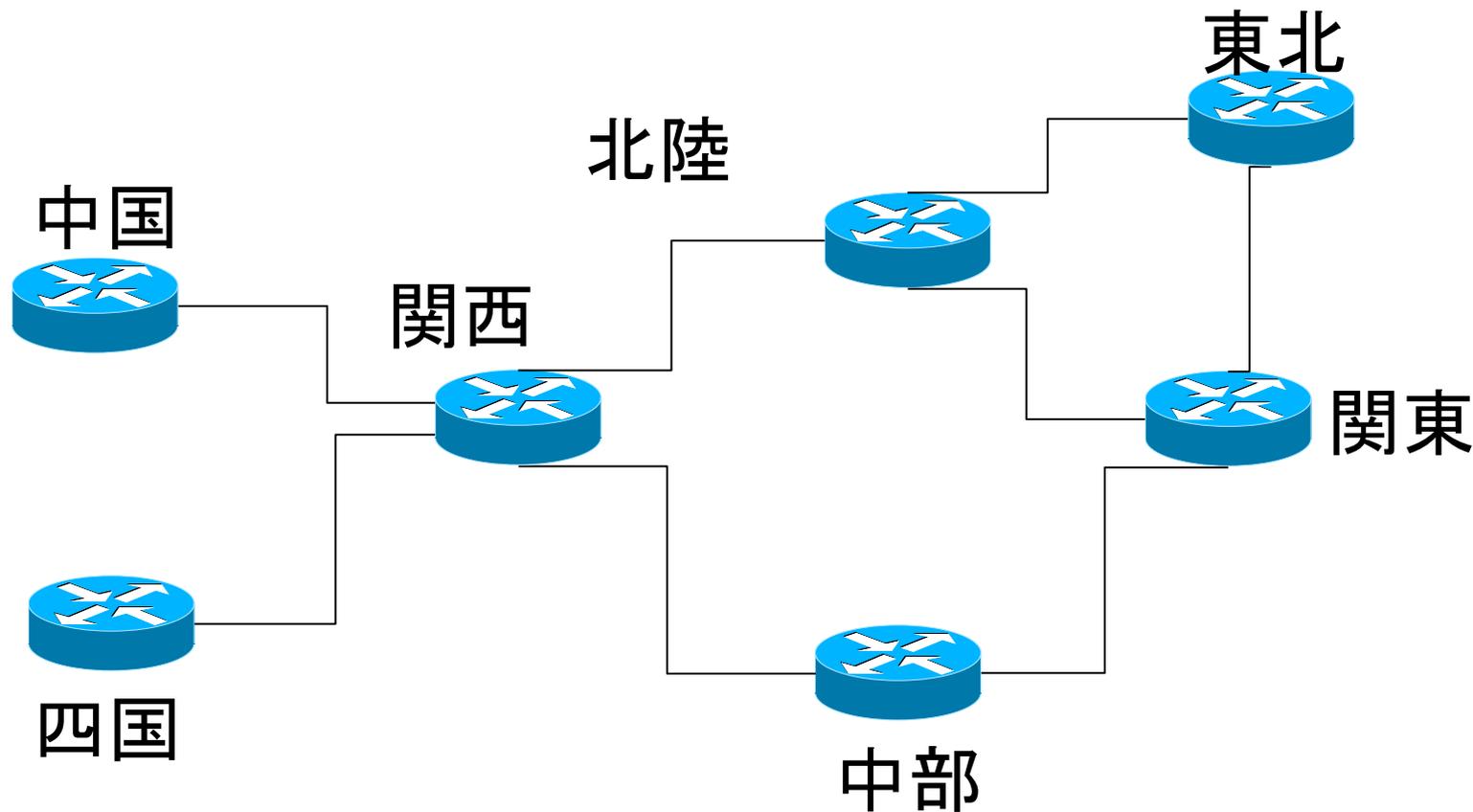
単純なトラフィック統計
(MRTG等)

xFlow

ケース1

拠点間通信の内訳がみたい

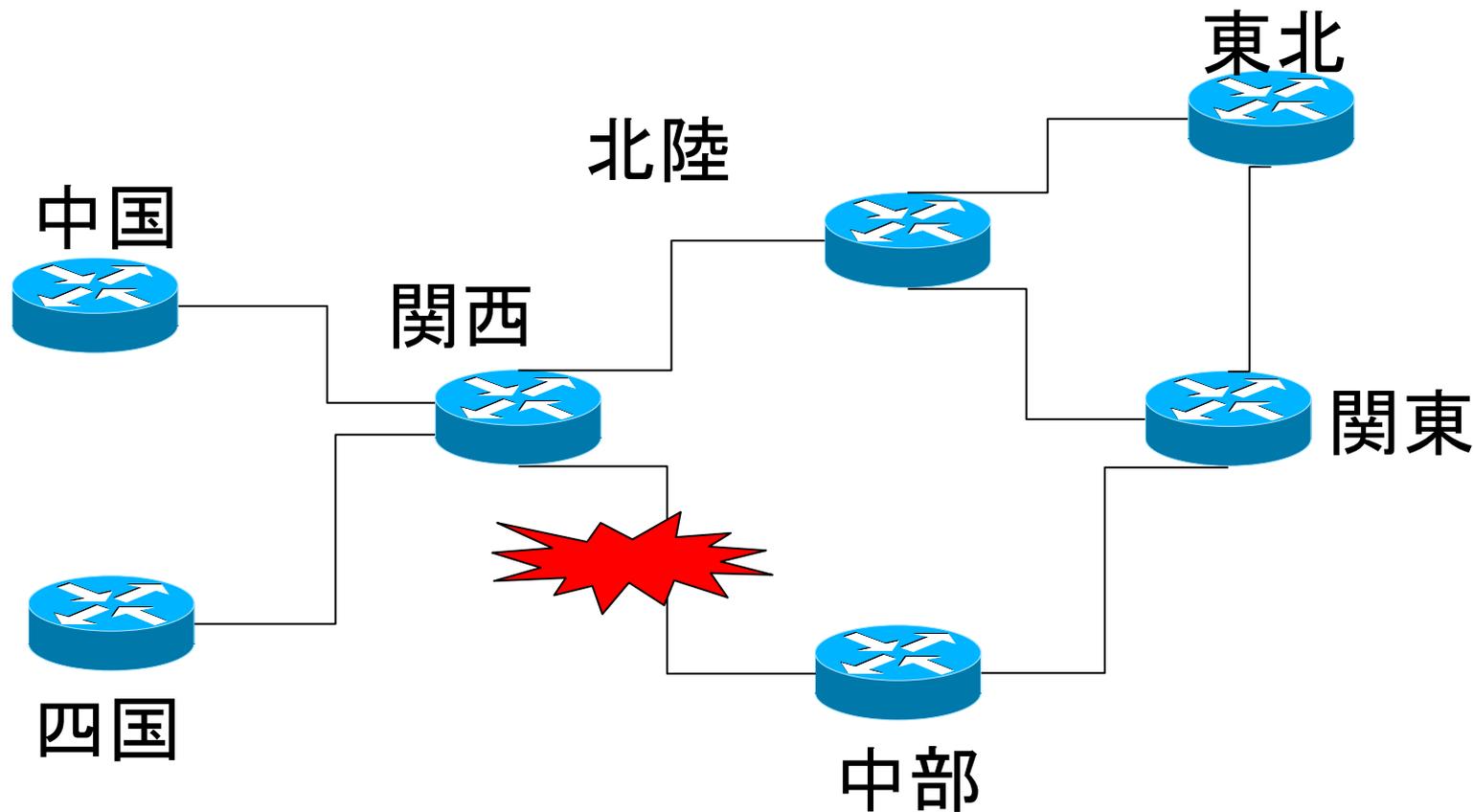
□ 例えばこんなネットワーク



ケース1

拠点間通信の内訳がみたい

□ 中部～関西が輻輳したら・・・



ケース1

拠点間通信の内訳がみたい

□ 単純なトラフィック統計の場合

→ 溢れている事はわかる

→ 「関西宛が多い」のか

「中国宛が多い」のか

「四国宛が多い」のか

「実は東側への迂回」なのかは

わからない

ケース1

拠点間通信の内訳がみたい

□ xFlowの場合

- Source/Destination IP Address
毎のトラフィックが集計可能
- 拠点毎のアドレスを把握しておけば、各拠点間の通信量が分かる

ケース2

ISPごとの通信量をみたい

□例えばこんなインターネット接続

- ✓ 高い上位ISP向け接続

- ✓ 安い Peering 向け接続

- ✓ いろいろなお客さんの接続

➔ いろいろ使い分けをしたい!

ケース2

ISPごとの通信量をみたい

□ 単純なトラフィック統計の場合

✓ 総量しか分からない

ケース2

ISPごとの通信量をみたい

□ xFlowの場合

- ✓ Source/Destination AS 毎のトラフィック集計が可能

ケース2

ISPごとの通信量をみたい

□AS番号?

- ✓ BGPで利用するルーティングドメイン毎に付ける番号
- ✓ 大きなISPには固有の番号がついていると思えばよい
- ✓ <http://www.nic.ad.jp/ja/ip/as-numbers.txt>

ケース2 ISPごとの通信量をみたい

AS番号リスト (2010/08/03現在)

*: JPNICに対して返却済みのもの



AS番号 AS名 連絡先

2497	IIJ	
2498*		
2499	ipv4exh-lab	
2500	WIDE-BB	
2501	TISK	
2502	TRAIN	
2503	TOPIC	
2504	NCA5	
2505	HEPNET-J	
2506	SuperCSI	
2507*		
2508	kyushu-u	
2509*		
2510	INFOWEB	
2511	CORE	
2512	TCP-NET	
2513	JST	
2514	InfoSphere	
2515	JPNIC	
2516	KDDI	
2517*		
2518	BIGLOBE	

ブドメ

がつ

)/as-

ケース2

ISPごとの通信量をみたい

□使い道1

- 高い上位ISP接続でトラフィック量の多いASを探す
- ➔ 安いPeering接続への移行や、お客さんとしての取り込みをはかる
- ➔ しあわせ :)

ケース2

ISPごとの通信量をみたい

□使い道2

- 自分やお客さんのAS向けのトラフィックが多いISPを探して営業をかける
- ➔ そういうお客さんなら割引して売っても元が取れる
- ➔ しあわせ :)

ケース3

DDoSの中身を見たい

□単純なトラフィック統計の場合

- 1Hop毎に「どこから」「どこへ」行っているかを確認める
- 結局packet captureしなくてははいけない :(

ケース3

DDoSの中身を見たい

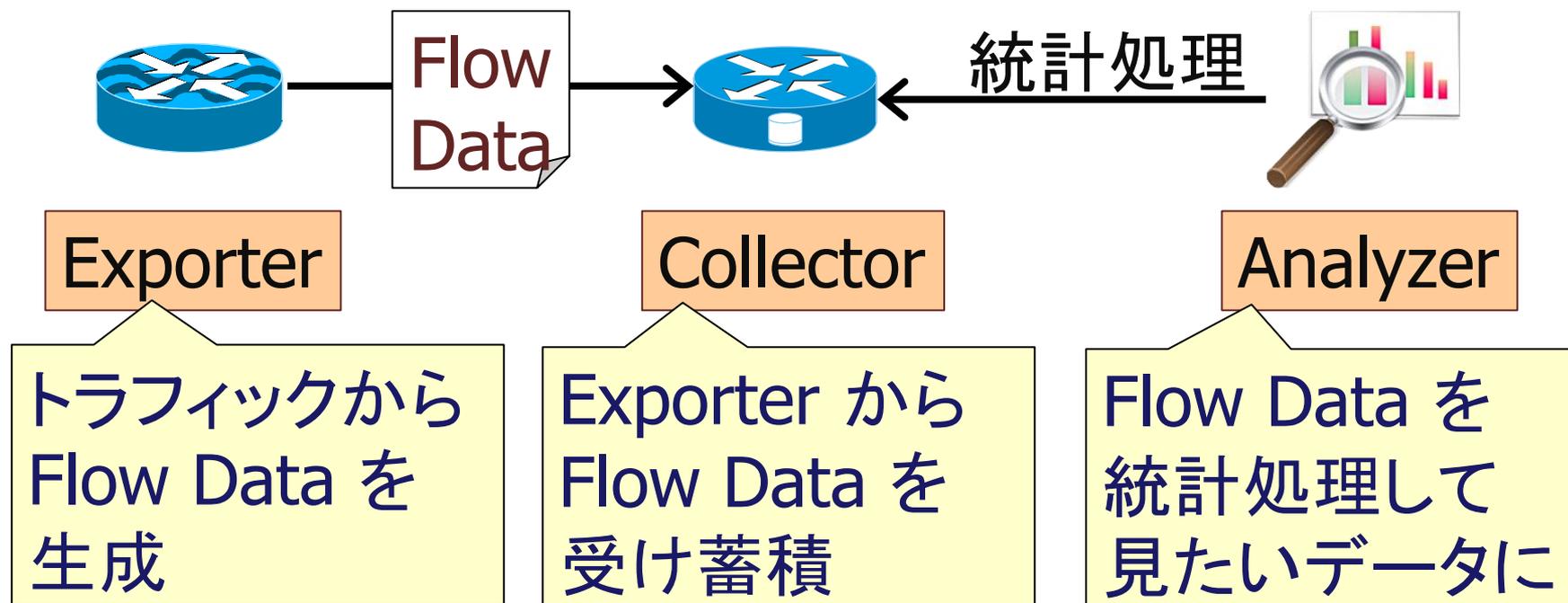
□xFlowの場合

- ✓ どんなIPアドレスから
- ✓ どんなAS (ISP)から
- ✓ どんなプロトコルで

来ているかくらいは取得しているフローデータからすぐ出せる：)

ツールの紹介

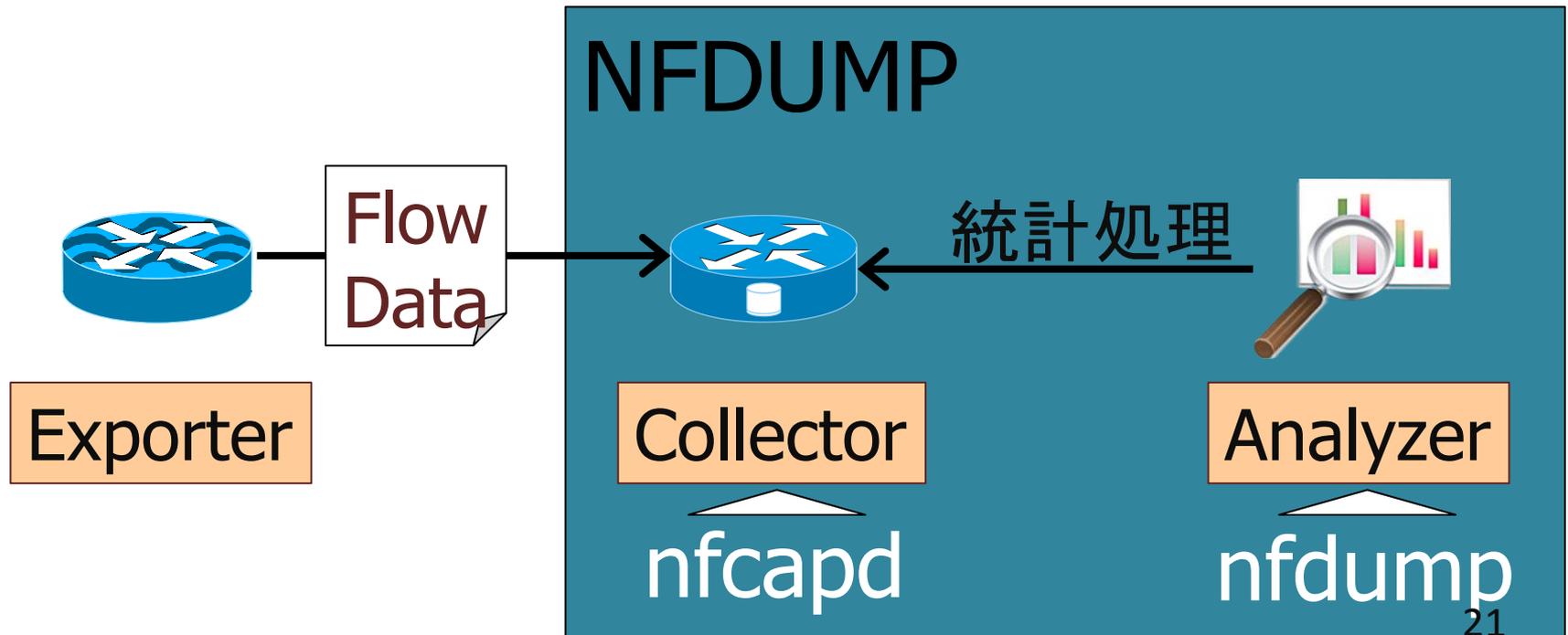
□ xFlowの構成要素



ツールの紹介

NFDUMP

□ <http://nfdump.sourceforge.net>



ツールの紹介

NFDUMP

□特徴

- CUIベースのAnalyzerと、Collector のシンプルな構成
- データを加工して見たいデータを抽出するのに向いている
- きちんとメンテされている【重要】

ツールの紹介

NFDUMP

□ FlowDataを見してみる

➤ `nfdump -r FILE`

ツールの紹介

NFDUMP

□ フローの数だけ表示される :-

```
Date flow start      Duration Proto      Src IP Addr:Port    Dst IP Addr:Port    Packets  Bytes  Flows
2010-08-05 20:34:15.134      0.000 UDP        192.168.0.1:161    -> 172.16.0.1:45087     10      1120   1
2010-08-05 20:34:02.054      0.000 UDP        192.168.0.1:161    -> 172.16.0.1:45030     10      1120   1
2010-08-05 20:34:02.054      0.000 UDP        192.168.0.1:161    -> 172.16.0.1:45034     10      1120   1
2010-08-05 20:34:40.622      0.000 UDP        192.0.2.1:53       -> 172.30.0.53:56674    10      1340   1
2010-08-05 20:34:33.163      0.000 UDP        10.0.0.1:35406     -> 172.30.53.53:53      10       720   1
2010-08-05 20:34:41.874      0.000 UDP        10.10.10.10:53     -> 172.30.0.53:59577    10      1460   1
2010-08-05 20:34:42.016      0.000 UDP        10.99.10.10:53    -> 172.30.0.53:51656    10      1930   1
2010-08-05 20:34:34.036      0.000 UDP        192.168.100.1:53   -> 172.30.0.53:37725    10      4870   1
2010-08-05 20:34:48.863      0.000 ICMP      10.100.100.200:0   -> 172.16.0.2:8.0      10       840   1
2010-08-05 20:34:52.201      0.000 UDP        10.200.200.100:53 -> 172.30.0.53:57756    10       690   1
2010-08-05 20:34:20.927      0.000 ICMP      172.16.0.3:0       -> 172.25.0.228:0.0    10       840   1
2010-08-05 20:34:02.360      0.000 UDP        172.16.0.16:161   -> 172.25.1.248:50241   10      1560   1
2010-08-05 20:34:13.561      0.000 UDP        172.20.0.20:15996 -> 172.30.53.53:53     10      1750   1
2010-08-05 20:34:46.621      0.000 UDP        192.168.255.254:60150 -> 172.30.53.53:53     10      1740   1
2010-08-05 20:34:18.098      0.000 TCP        10.25.25.25:63292 -> 172.25.25.25:25     10       480   1
2010-08-05 20:34:19.424      0.000 TCP        10.25.25.25:63292 -> 172.25.25.25:25     10       640   1
~~snip~~
Summary: total flows: 31959, total bytes: 109377120, total packets: 437020, avg bps: 2433854, avg pps: 1215, avg
bpp: 250
Time window: 2010-08-05 20:33:55 - 2010-08-05 20:39:54
Total flows processed: 31959, Blocks skipped: 0, Bytes read: 1661908
Sys: 0.460s flows/second: 69476.1   Wall: 0.444s flows/second: 71970.7
```

ツールの紹介

NFDUMP

□ raw形式で表示してみる

➤ `nfdump -o raw -r FILE`

ツールの紹介

NFDUMP

□ フローの詳細が表示される :)

```
Flow Record:
Flags           =          0x80  Sampled
size           =             52
first          =    1281008071  [2010-08-05 20:34:31]
last           =    1281008071  [2010-08-05 20:34:31]
msec_first     =             464
msec_last     =             464
src addr       =          10.0.0.1
dst addr       =         192.168.0.1
src port       =             53
dst port       =          25565
fwd status     =             0
tcp flags      =          0x00  .....
proto          =             17
(src)tos       =             0
(in)packets    =             10
(in)bytes      =          1190
input          =             37
output         =             36
src as         =          64512
dst as         =          65535
```

ツールの紹介

NFDUMP

□ Top Talker を抽出してみる

➤ `nfdump -s srcip/bytes -n 10`

ツールの紹介

NFDUMP

□ 暴れん坊がすぐ見つかる :D

```
$ nfdump -s srcip/bytes -n 10 -r nfcapd.XXXXXXXXXXXXXX
Top 10 Src IP Addr ordered by bytes:
Date first seen      Duration Proto      Src IP Addr      Flows(%)      Packets(%)      Bytes(%)      pps      bps
2010-08-05 20:48:56.002    299.956 any        10.100.10.1      11( 0.0)      32720( 7.9)    48719830(43.5)  109    1299386
2010-08-05 20:48:56.221    299.480 any        192.168.1.1      8( 0.0)       11060( 2.7)    15929060(14.2)   36    425512
2010-08-05 20:48:56.002    359.331 any        172.16.0.100     3143(10.0)    34330( 8.2)    4975150( 4.4)   95    110764
2010-08-05 20:48:55.995    298.478 any        192.0.2.100      81( 0.3)       3660( 0.9)     4697670( 4.2)   12    125909
2010-08-05 20:49:01.899    239.919 any        192.0.2.200      65( 0.2)       3130( 0.8)     3739100( 3.3)   13    124678
2010-08-05 20:49:55.287    300.236 any        10.10.10.10      2181( 7.0)    24670( 5.9)    3546600( 3.2)   82    94501
2010-08-05 20:48:55.998    299.956 any        192.168.100.1    1132( 3.6)    23190( 5.6)    1488370( 1.3)   77    39695
2010-08-05 20:48:55.993    299.033 any        172.20.0.254     909( 2.9)     10610( 2.5)    1440720( 1.3)   35    38543
2010-08-05 20:48:58.622    296.157 any        192.168.20.1     169( 0.5)      2050( 0.5)    1397450( 1.2)   6     37748
2010-08-05 20:53:06.502      1.108 any         10.1.1.1         13( 0.0)       620( 0.1)     857240( 0.8)   559   6189458

Summary: total flows: 31330, total bytes: 111901950, total packets: 416370, avg bps: 2489953, avg pps: 1158, avg bpps: 1158
Time window: 2010-08-05 20:48:55 - 2010-08-05 20:54:55
Total flows processed: 31330, Blocks skipped: 0, Bytes read: 1629200
Sys: 0.040s flows/second: 783250.0  Wall: 0.035s flows/second: 890638.8
```

ツールの紹介

NFDUMP

□ フォーマットを定義してみる

- SrcAS/DstAS毎のトラフィック量をCSVに

ツールの紹介

NFDUMP

- HTML化やグラフ化もちよっとがんばればできる :)

```
$ nfdump -q -s record/packets -n 10 -A srcas,dstas -o "fmt:%sas,%das,%byt,%pkt" -r nfcapd.xxx
64600, 64512, 3185900, 47760
64600, 65535, 2984050, 44200
65000, 65000, 53014030, 39370
64600, 65535, 2048410, 27920
65535, 64600, 2749160, 19680
64512, 64600, 2029530, 14550
64512, 65000, 15959120, 11180
64500, 65535, 766750, 10320
64500, 64512, 722430, 9680
64700, 65000, 2888860, 6460
```

↑ ↑ ↑ ↑
Source AS Destination AS byte count packet count

ツールの紹介

Nfsen

- <http://nfsen.sourceforge.net>
 - NFDUMPのWebフロントエンド

ツールの紹介

Nfsen

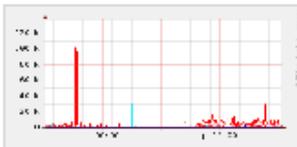
□ Nfsenで見えること

- ICMP,TCP,UDP別のFlow数
- UDP,TCP port毎のFlow分布
- Top N Talker

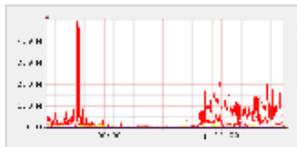
ツールの紹介

Nfsen

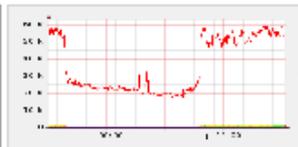
TCP Packets



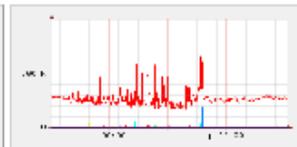
TCP Bytes



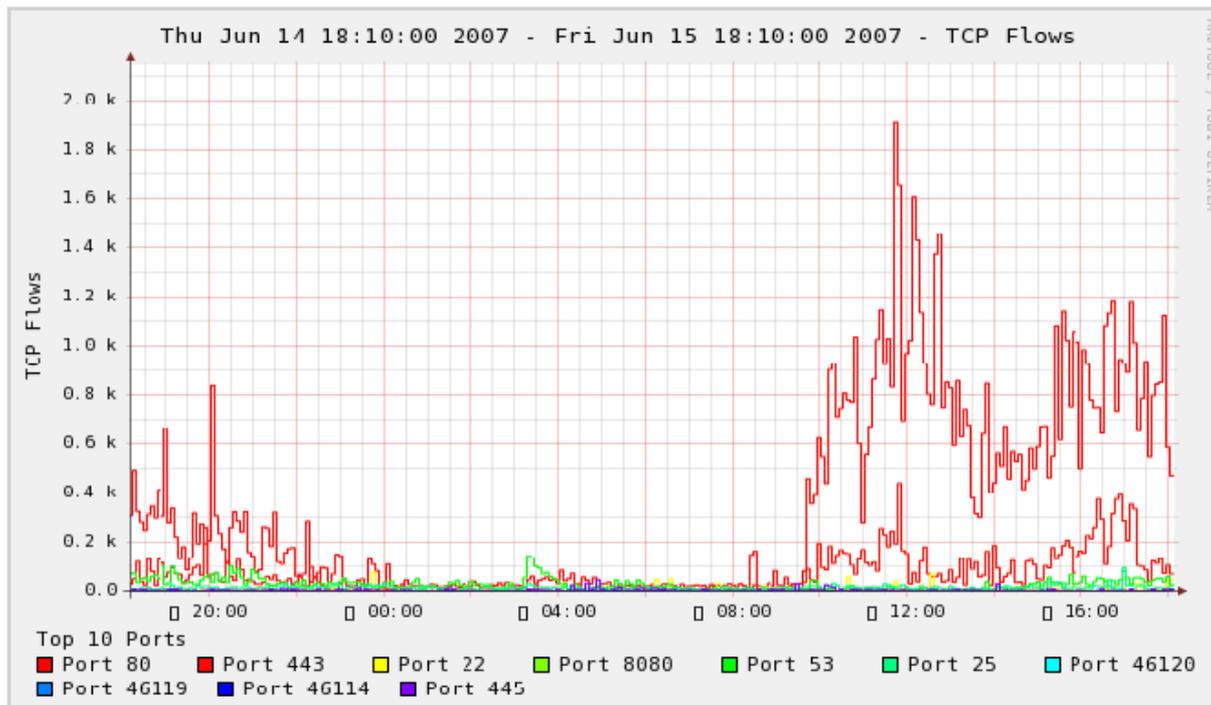
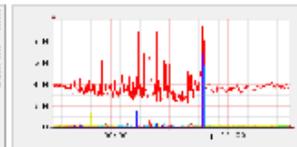
UDP Flows



UDP Packets



UDP Bytes



Show Top Ports

now 24 hours

Track Ports:

Add

Delete

Skip Ports:

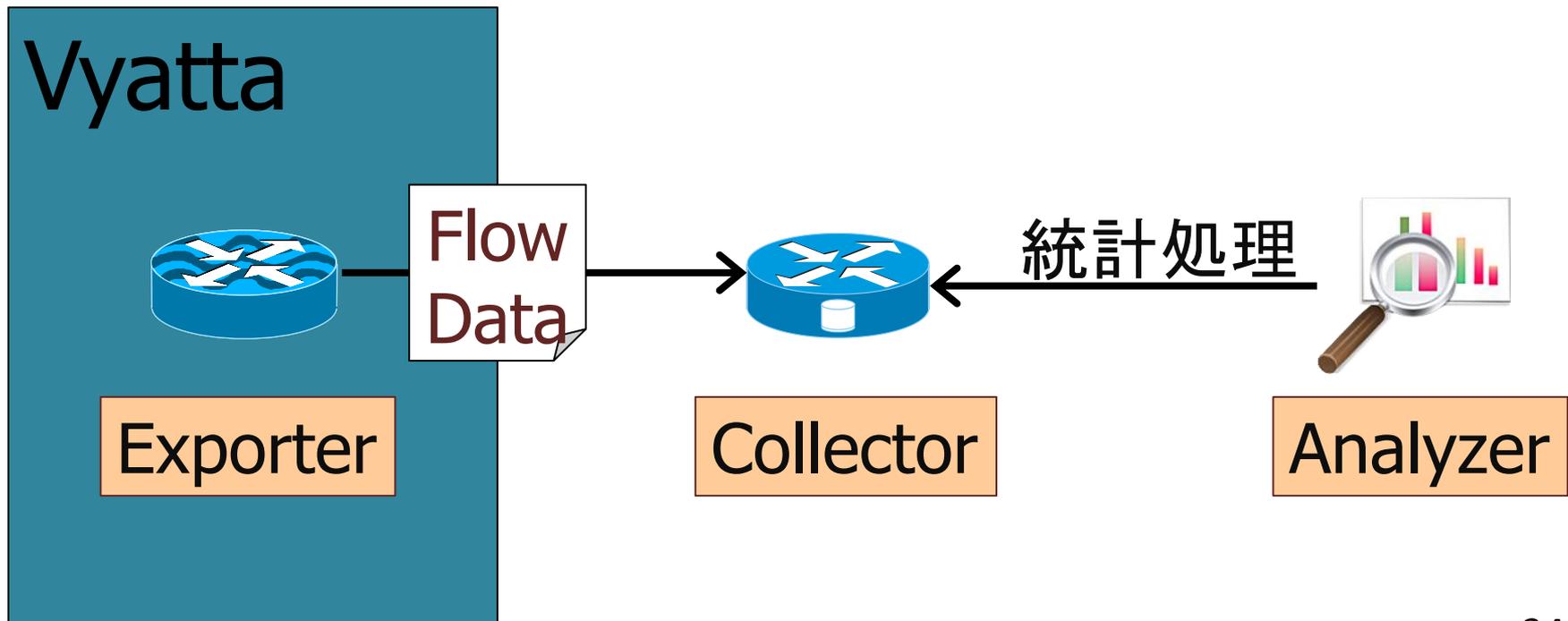
Add

Delete

ツールの紹介

Vyatta

□ <http://www.vyatta.com/>



ツールの紹介

Vyatta

□ ソフトウェアルータ

- BGPもOSPFも xFlow も動く :)
- VC6以降で NetFlow v1,5,9 及び sFlow に対応
- 日本のユーザ会もできて活発
 - ✓ <http://www.vyatta-users.jp/>

ツールの紹介 Vyatta

特集1



銀座堂の石本 勝一(左)さんと
浅間 正和(右)さん

銀座堂が提供するインターネット接続サービス「GINZADO-NET」のネットワークを運用している。

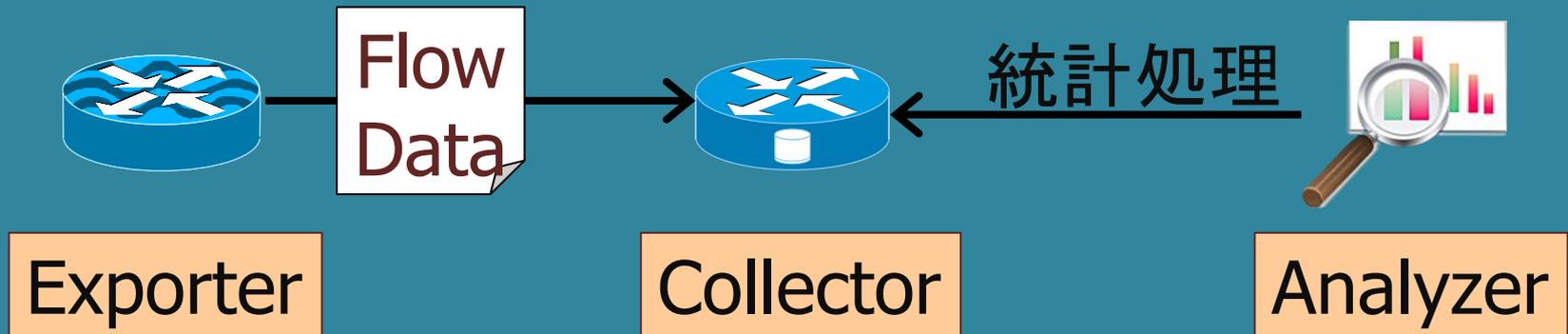
触って学ぶ
ルーター&VPN

ツールの紹介

ntop

□ <http://www.ntop.org/>

Ntop



ツールの紹介

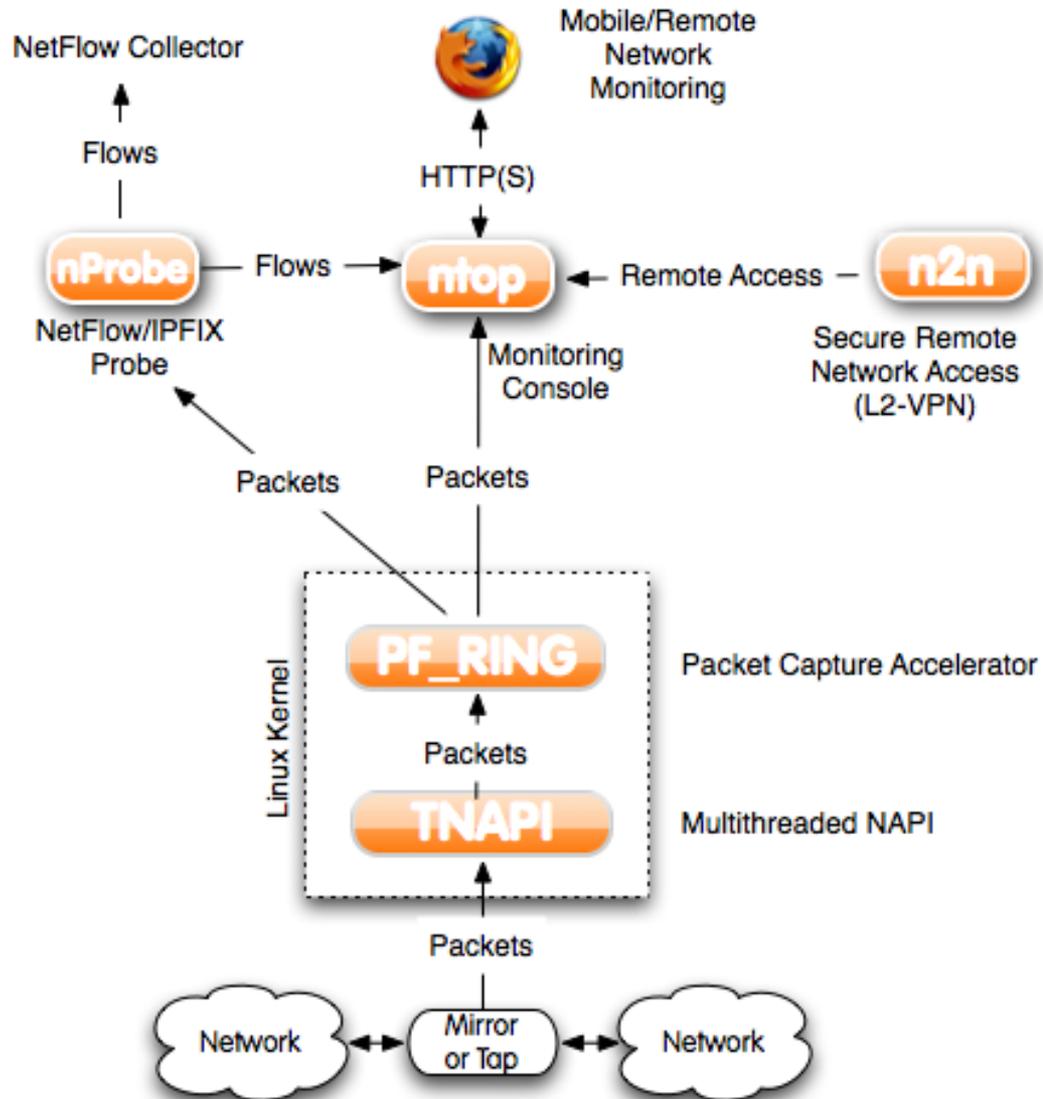
ntop

□ とにかくお手軽

- ExpoterからAnalyzerまで全部。
- xFlowを使わなくても、ローカルを pcap ベースで見ただけです
ごい。。。

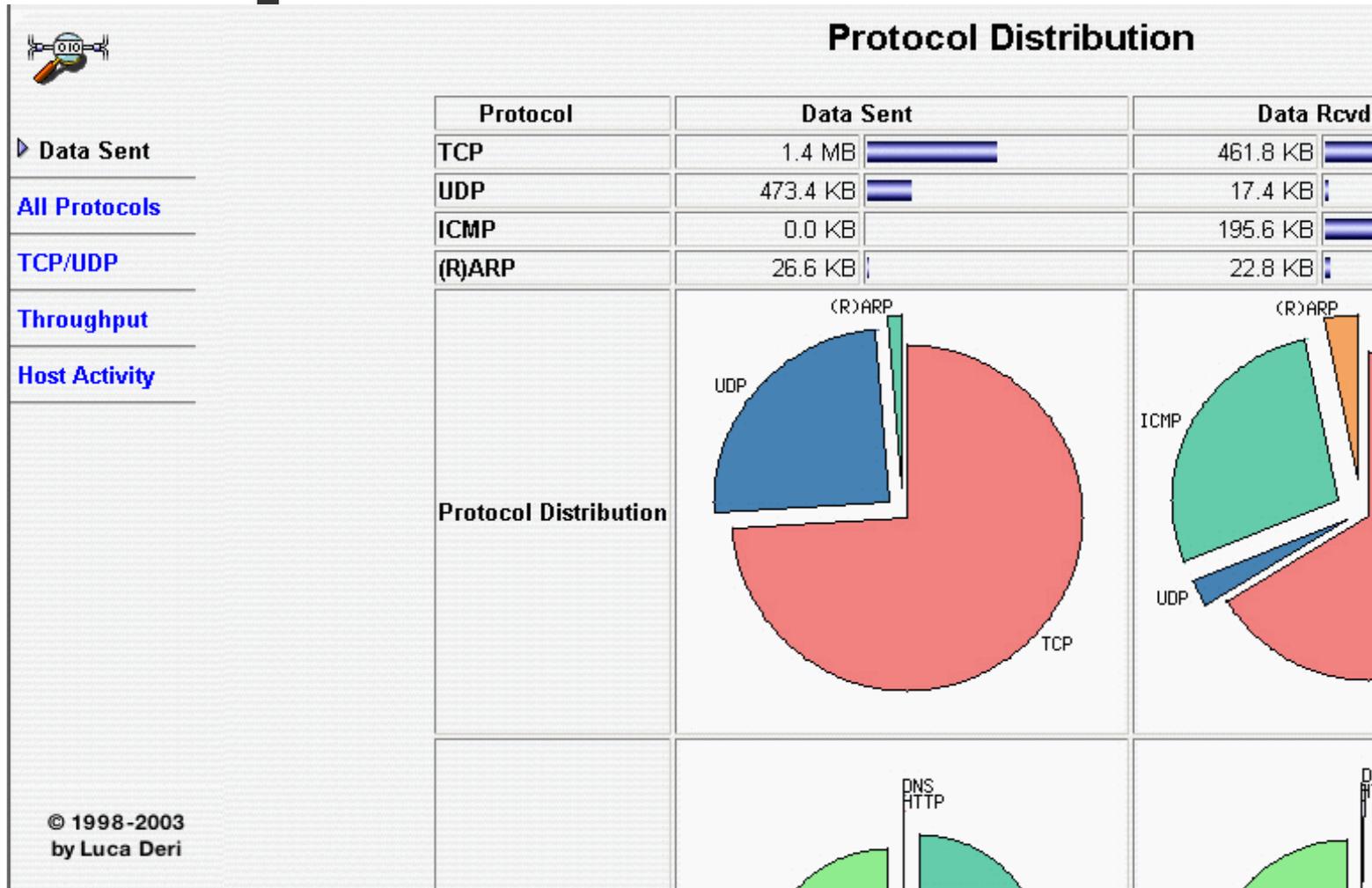
ツールの紹介

ntop



ツールの紹介

ntop



ツールの紹介

ntop

Welcome to ntop: [About](#) | [Summary](#) | [IP Summary](#) | [All Protocols](#) | [Local IP](#) | [FC](#) | [SCSI](#) | [Admin](#) | (C) 1998-2004 - L. Deri

All Protocols: [Traffic](#) | [Throughput](#) | [Activity](#)

Network Traffic [All Protocols]: All Hosts - Data Sent+Received

Hosts: [All] [Local Only] [Remote Only]

Data: [All] [Sent Only] [Received Only]

Host	Domain	Data	TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP	AppleTalk	NetBios	OSI
alb-24-29-56-1.nycap.rr.com		12.1 MB 35.0 %	0	0	0	0	0	0	0	12.1 MB	0	0	0
alb-24-194-134-127.nycap.rr.com		11.1 MB 32.0 %	10.8 MB	244.8 KB	13.3 KB	0	0	0	0	46	0	0	0
www.oasis-open.org		8.2 MB 23.7 %	8.2 MB	0	0	0	0	0	0	0	0	0	0
www.winnetmag.com		233.4 KB 0.7 %	233.4 KB	0	0	0	0	0	0	0	0	0	0
albny-dns-cac-02-dmfe1.nyroc.rr.com		227.6 KB 0.6 %	0	227.6 KB	0	0	0	0	0	0	0	0	0
www.freeware-base.de		193.9 KB 0.5 %	193.9 KB	0	0	0	0	0	0	0	0	0	0
www.snort.org		189.4 KB 0.5 %	189.4 KB	0	0	0	0	0	0	0	0	0	0
ads.osdn.com		144.7 KB 0.4 %	144.7 KB	0	0	0	0	0	0	0	0	0	0
icons.wunderground.com		130.2 KB 0.4 %	130.2 KB	0	0	0	0	0	0	0	0	0	0
sourceforge.net		122.6 KB 0.3 %	122.6 KB	0	0	0	0	0	0	0	0	0	0
ms-pop-00.nycap.rr.com		115.2 KB 0.3 %	115.2 KB	0	0	0	0	0	0	0	0	0	0
www.juanso.com		111.6 KB 0.3 %	111.6 KB	0	0	0	0	0	0	0	0	0	0
www.wabbit1.homestead.com		102.6 KB 0.3 %	102.6 KB	0	0	0	0	0	0	0	0	0	0
205.188.12.16		102.4 KB 0.3 %	102.4 KB	0	0	0	0	0	0	0	0	0	0

実用上の諸注意

□ xFlow のイケてるところばかりを紹介してきましたが、

気をつけなくてはならないこともたくさん……

実用上の諸注意

□データ保存形式

- xFlowの生データは巨大
- ➔ トラフィック量によってはいくらストレージがあっても足りない
- ➔ 短期間は生データで保存し、長期間は整形したデータのみを保存する等、工夫が必要。

実用上の諸注意

□ サンプルング

- 全てのパケットフローを xFlow で Exportするのは大変
- ➔ トラフィックの傾向を把握する用途なら、サンプルングしたデータでも十分。

実用上の諸注意

□最後に・・・

- 売りモノに較べるとイケてる Presenter の実装は多くない
- 結局、nfdump や flow-tools 等を使って作り込みをしているISPが多いのが実状
- 是非、情報交換しましょう！)