

Practical Experience with IPFIX Flow Collectors

Petr Velan
petr.velan@cesnet.cz

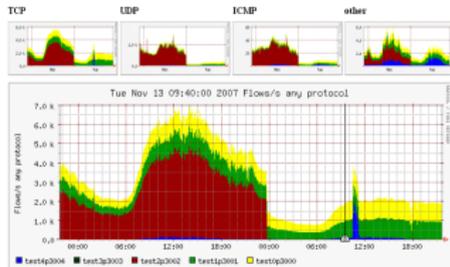


IFIP/IEEE IM 2013, 27-31 May 2013
Ghent, Belgium

Introduction

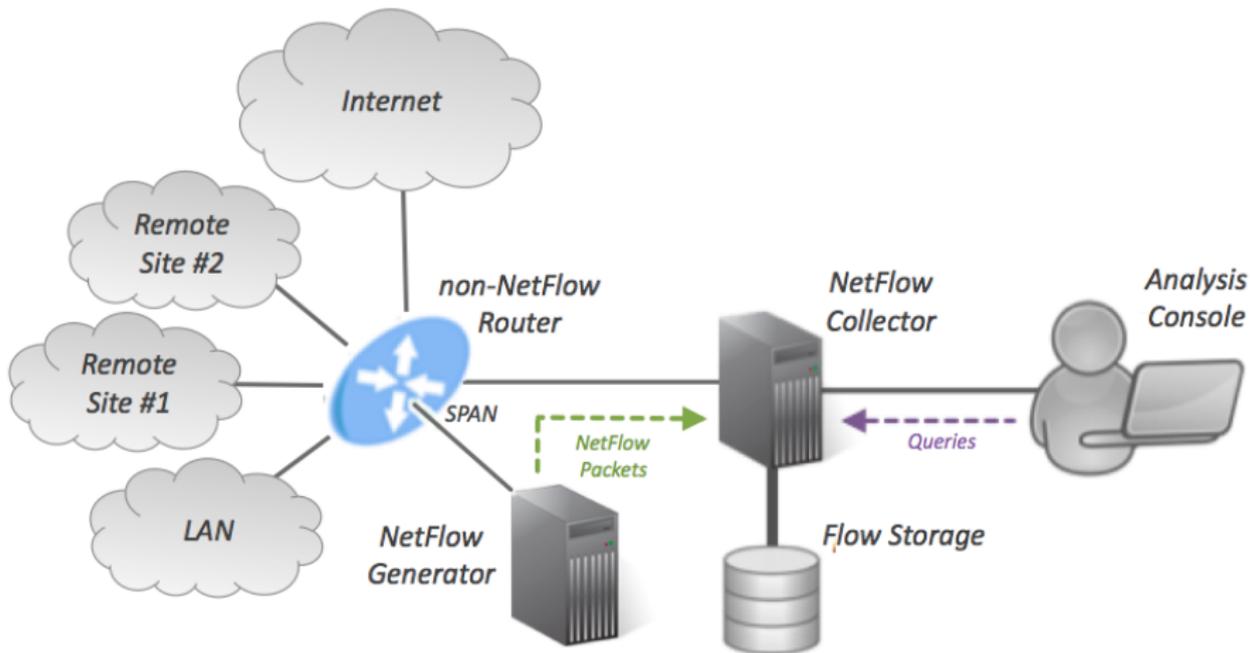
NetFlow Measurement

- Network monitoring is an essential tool for security
- 10Gbps lines are quite common
- Flow monitoring becomes widely used
- NetFlow version 5, 9, 10 -> IPFIX



Introduction

NetFlow Measurement Schema



Schema from <http://plexer.com>

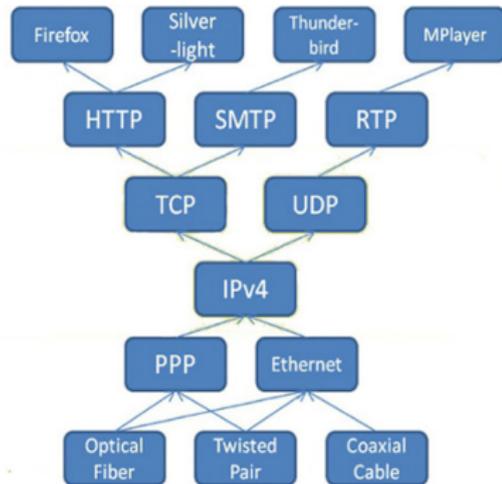
Introduction

NetFlow example (nfdump output)

Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Packets	Bytes
2013-04-25 07:59:01.488	30.001	TCP	195.113.182.45:49169	->	173.194.70.125:5222	3	226
2013-04-25 07:58:47.441	36.622	TCP	193.170.162.118:4621	->	173.194.35.78:443	7	281
2013-04-25 07:59:29.595	0.169	TCP	145.244.10.3:47924	->	173.194.40.31:80	6	1010
2013-04-25 07:59:20.324	0.748	TCP	195.113.158.86:53647	->	173.194.70.95:80	6	907
2013-04-25 07:59:28.663	0.000	TCP	193.87.81.2:2989	->	173.194.35.72:80	2	80
2013-04-25 07:59:01.508	21.194	TCP	91.210.16.190:179	->	91.210.16.62:17045	2	147
2013-04-25 07:59:23.884	0.295	TCP	195.113.201.101:50759	->	173.194.35.70:80	2	936
2013-04-25 07:59:01.513	27.311	TCP	91.210.16.190:179	->	91.210.16.109:8220	2	147
2013-04-25 07:59:01.515	18.030	TCP	91.210.16.190:179	->	91.210.16.205:48598	2	99
2013-04-25 07:59:01.514	23.094	TCP	91.210.16.190:179	->	91.210.16.97:46878	2	147

Motivation

- New tasks for flow monitoring:
 - Non-IP networks
 - High-speed networks
 - Very different and specific systems
 - Application visibility
- NetFlow version 9 is too limited to fit every scenario
- IPFIX should be the solution



Motivation

IPFIX Protocol

- Enterprise elements
- Variable length fields
- Support of connection oriented protocols: TCP, SCTP
- TLS, DTLS
- Lack of IPFIX collector frameworks

Motivation

Goals

- Find open-source IPFIX collection frameworks
- Determine the level of provided IPFIX support
- Compare a performance of query tools
- Extensibility of query tools



Open Source IPFIX frameworks

- nTop, nProbe
 - Exporter with additional support
- nfdump
 - Data capture tool, query tool
- SiLK
 - Tools for small tasks
- Vermont
 - One XML configurable tool
- IPFIXcol
 - Like nfdump, XML configuration

IPFIX Elements Support

Element	ndump	SiLK	Vermont	IPFIXcol
Reverse elements	no	no	yes	yes
Flow end reason	no	yes	no	yes
Vlan ID	yes	yes	no	yes
Next hop IP	yes	yes	no	yes
Forwarding status	yes	no	no	yes
SNMP	yes	no	no	yes
Autonomous sys.	yes	no	no	yes
MPLS	yes	no	no	yes
Exporter IP	yes	no	no	yes
BGP Next Hop IP	yes	no	no	yes
Mac addresses	yes	no	no	yes
Flow direction	yes	no	no	yes
Enterprise elements	no	limited	no	yes

Collection Frameworks extensibility

- Vermont uses relational database
- SiLK has IPv6 support determined at compilation time
- nfdump uses templates
- IPFIXcol uses XML configuration
FastBit database for data storage

Query Tool Performance

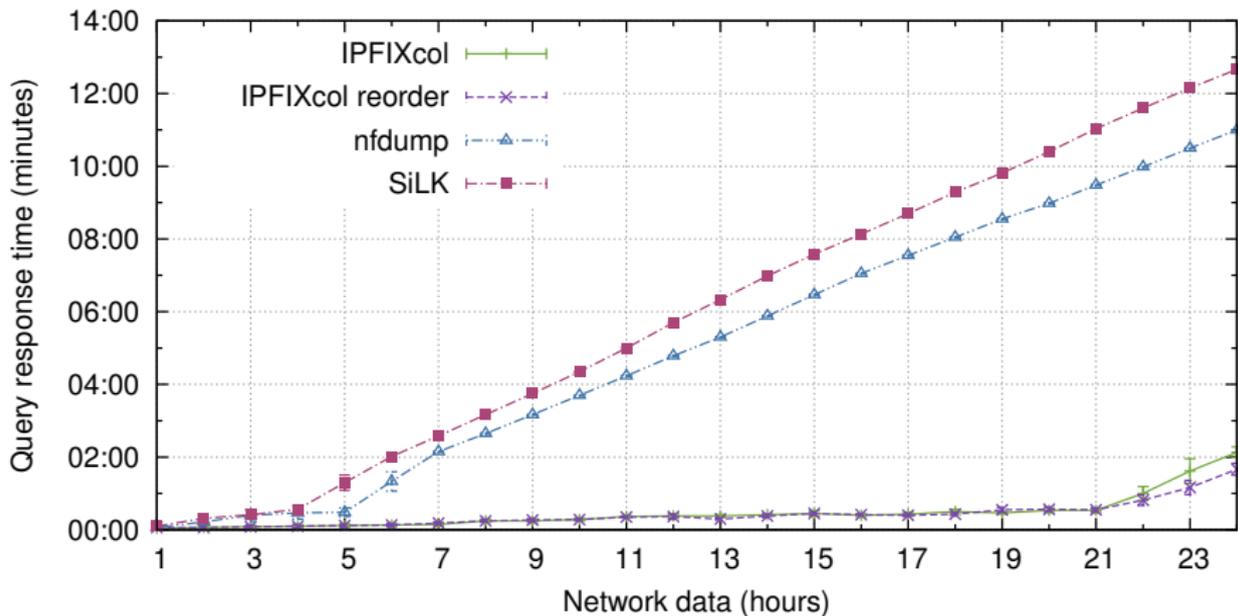
Data Set

- 1 day network data sample
- Almost 1.1 billion flows
- 52.7 GB data size in nfdump format (without compression)
- 52.7 GB data size in IPFIXcol format (+ 6.5 GB or 1.7 GB indexes)
- 67.2 GB data size in SiLK format



Query Tool Performance

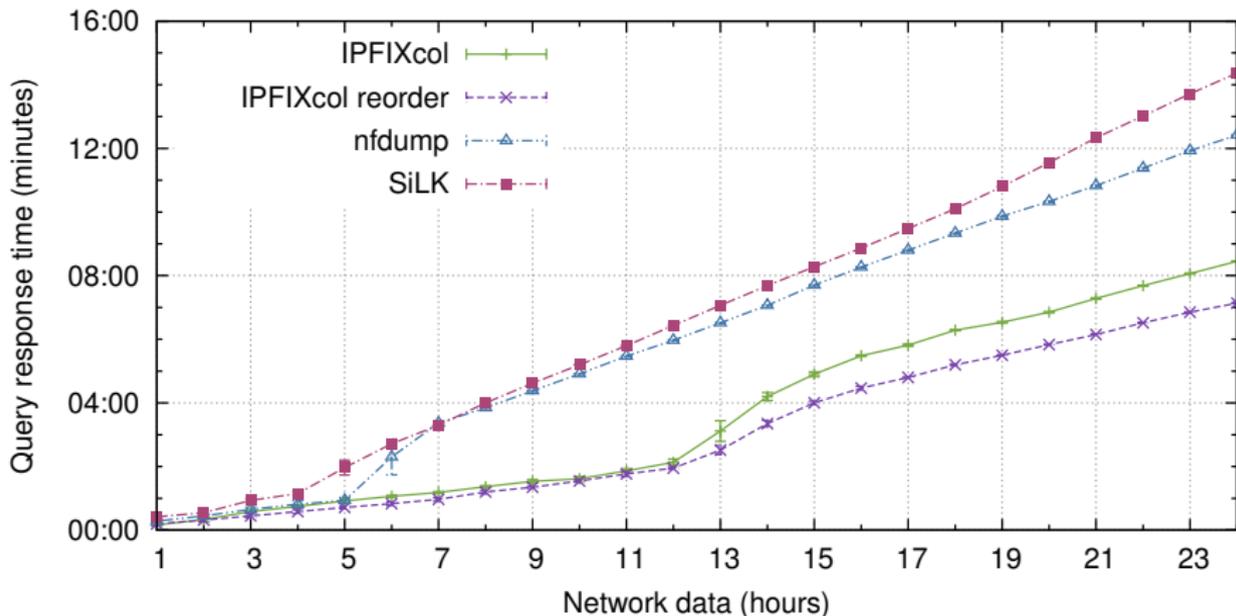
Q1



- SELECT count(*), sum(packets), sum(bytes) FROM dataset

Query Tool Performance

Q4



- `SELECT src_IPv4, packets, bytes, count(*) FROM dataset WHERE ip_version = 4 GROUP BY src_IPv4 ORDER BY bytes DESC LIMIT 5`

Query Tools Extensibility

- *IPFIXcol* has the IPFIX elements defined in XML
- *SiLK* allows its tools to be extended by Python plugins
- *nfdump* does not have any mechanism for extension

Conclusions

- There is a lot of work to do in the field of IPFIX collection frameworks
- It is difficult to add new IPFIX element to current frameworks
- Data storage format is of utmost importance

Thank You for Your Attention



Practical Experience with IPFIX Flow Collectors

Petr Velan

`petr.velan@cesnet.cz`

`https://www.liberouter.org`

