Monitoring of Tunneled IPv6 Traffic Using Packet Decapsulation and IPFIX

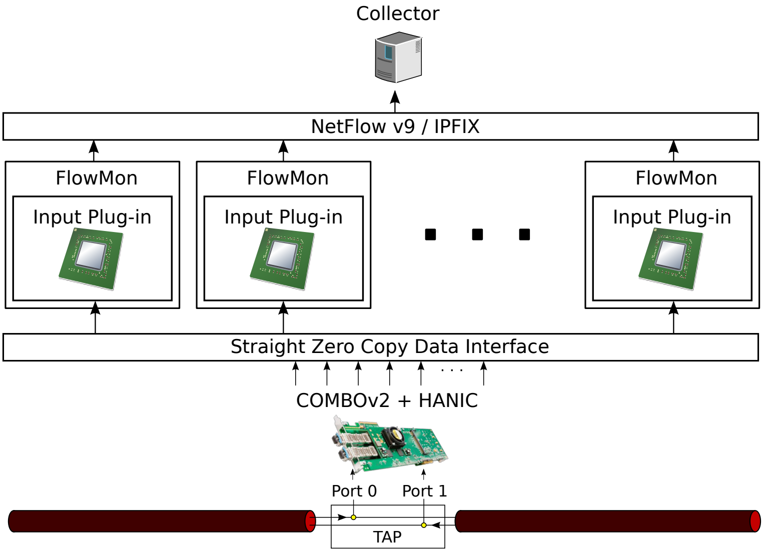
Martin Elich[1], Matěj Grégr[2] and Pavel Čeleda[1]

Masaryk University, Brno, Czech Republic – elich|celeda@mail.muni.cz

Brno University of Technology, Brno, Czech Republic – igregr@fit.vutbr.cz

Wien, 28th April 2011

Architecture of Monitoring Solution I



Architecture of Monitoring Solution II

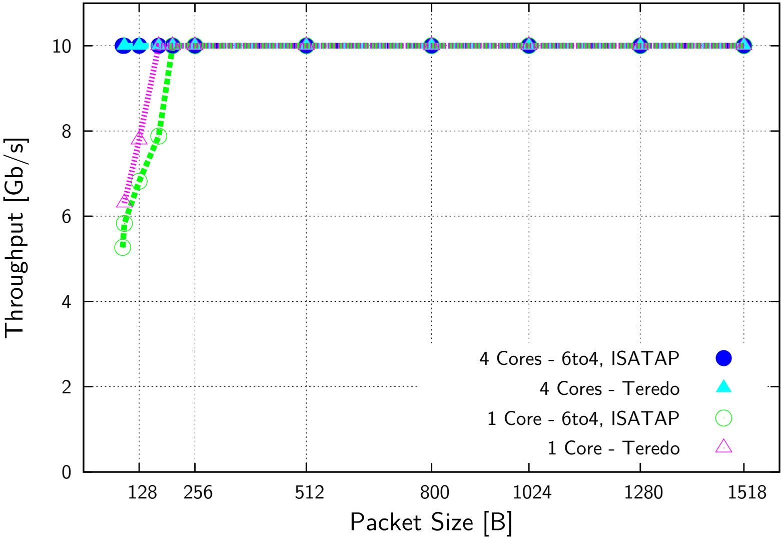
FlowMon exporter

- Generator of NetFlow/IPFIX data.
- Support of input plug-ins.

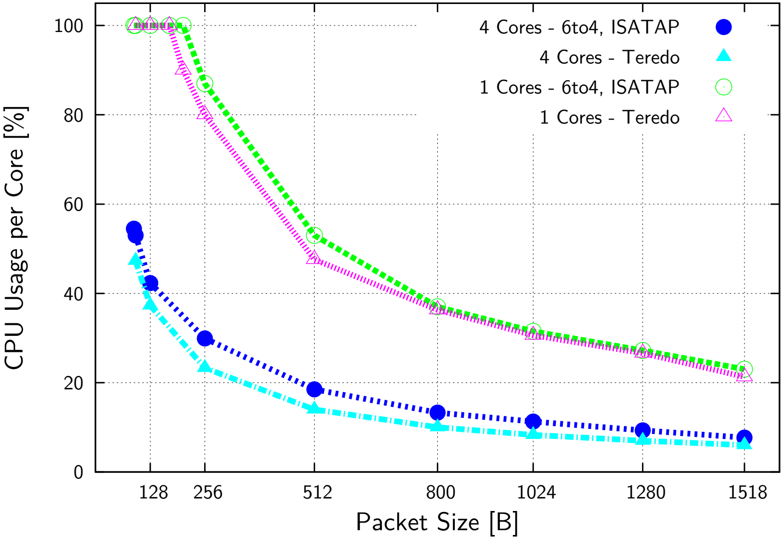
Input plug-in

- Detection and decapsulation of tunneled packets.
- Detection of used transiton mechanism.
- Extraction of outside and inside IP addresses.
- Extraction of outside and inside ports.

Throughput RFC2544



CPU Usage During the Test



Monitoring System

Data generating

- FlowMon exporter + plug-in → **NetFlow v9**.
- **Transport** of data to collector **over IPv6**.

Data collecting

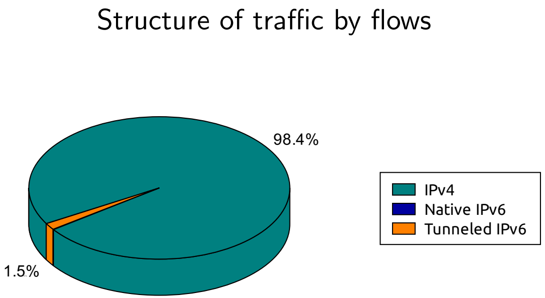
- **NfSen** 1.3.4 + **NFDUMP** 1.6.1.
- Enabled extensions 6 (src/dst vlan id labels).
- **Profiles**:
  - **native IPv6**,
  - **Teredo**,
  - **6to4**,
  - **ISATAP**.

Experiment

Testbed

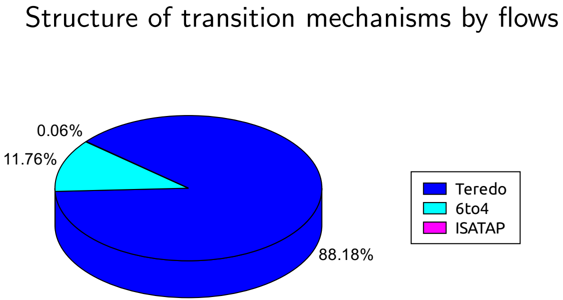
- Deployed on CESNET2 network.

Structure of Traffic



	Flows	Packets	Bytes
IPv4	98.39%	99.19%	99.13%
Native IPv6	0.10%	0.12%	0.21%
Tunneled IPv6	1.50%	0.69%	0.66%

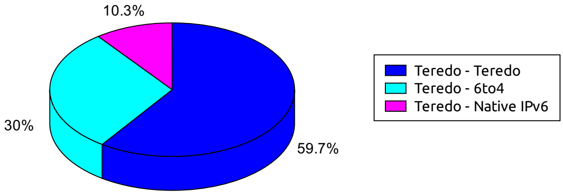
Structure of transition mechanisms in tunnels



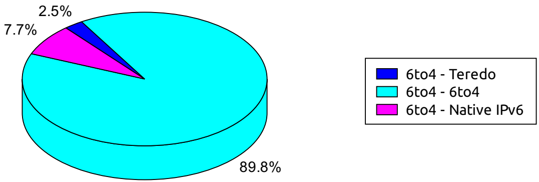
	Flows	Packets	Bytes
Teredo	88.18%	89.10%	88.85%
ISATAP	0.06%	0.03%	0.03%
6to4	11.76%	11.76%	11.12%

Targets of Communication in Teredo a 6to4 Tunnels

Teredo



6to4



Portion of HTTP, HTTPS a DNS Protocols

By Flows	IPv4	Native IPv6	Tunneled IPv6
HTTP	38.25%	1.99%	0.35%
HTTPS	3.26%	<0.01%	0.08%
DNS	10.39%	61.76%	0.45%

By Packets	IPv4	Native IPv6	Tunneled IPv6
HTTP	49.99%	65.50%	2.98%
HTTPS	1.72%	<0.01%	2.85%
DNS	0.45%	1.68%	0.05%

By Bytes	IPv4	Native IPv6	Tunneled IPv6
HTTP	56.80%	76.16%	0.38%
HTTPS	1.17%	<0.01%	0.33%
DNS	0.07%	0.42%	0.01%

Part I

Conclusion

Conclusion

Monitoring system

- **No equivalent** solution **found**.
- In future switching export from NetFlow to IPFIX.

Monitoring results

- **Tunneled** traffic **prevail over native** IPv6 traffic.
- **Different** structure of **traffic** in IPv6 tunnels and IPv4.
- **Majority** of traffic is generated by **P2P** networks and other **unidentified** services.