

SFLOW Analysis Tool

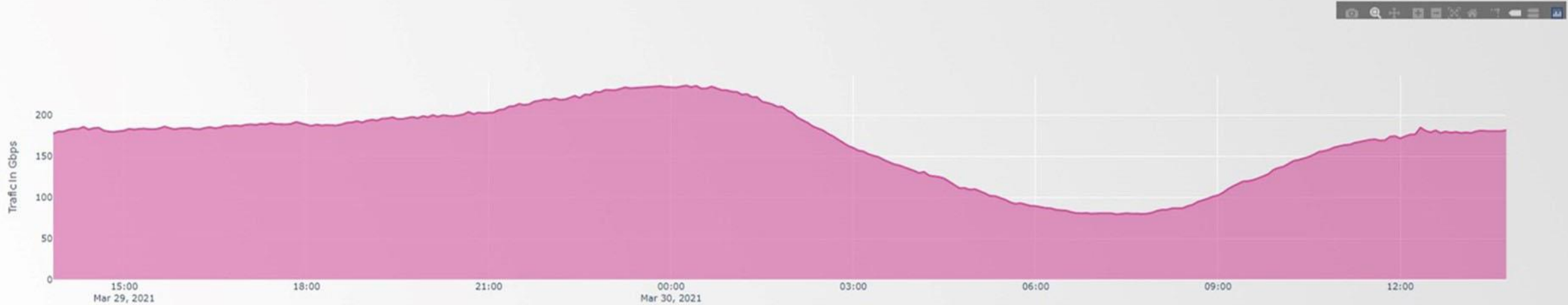
by Developico in cooperation with SOX (Serbian Open eXchange)



SFLOW Analysis Tool

- ❑ Traffic analysis tool based on SFLOW data
- ❑ Development in close cooperation with IXP experts
- ❑ Full stack software that uses only open-source program languages and frameworks
- ❑ Possibility for quick observation of traffic and network health as well as possibility for deep troubleshooting and fine tuning
- ❑ Special care of Privacy and GDPR through IP address anonymization
- ❑ Strong authentication method
- ❑ Uses pmacct as sflow collector (open-source software developed by Paolo Lucente)

Total traffic in Gbps, Daily



Top Vlans

Vlan ID	Name	Transferred
100	100	1.1 PB
101	101	200.2 TB
102	102	126.2 TB
103	103	104.0 TB

Interfaces table

Agent ID/ iface	Interface name	Transferred	Average Speed
10000	10000	245.0 TB	24.9476 gbps
10001	10001	242.6 TB	24.7020 gbps

Top Source AS → Destination AS pairs, vlan 304

Src AS	Dst AS	Transferred	Average Speed
10000	10000	251.9 TB	25.6409 gbps
10001	10001	67.7 TB	6.8900 gbps
10002	10002	48.4 TB	4.9232 gbps
10003	10003	46.8 TB	4.7634 gbps

Dashboard for data visualization:

- ❑ graph - total traffic
- ❑ by default, 24 hours
- ❑ predefined query Top VLANs, Interfaces, Top TCP ports, Top Source AS → Destination AS pairs

85.8 TB
81.9 TB
39.0 TB
31.6 TB
27.4 TB
23.7 TB

[see all...](#)

Top TCP Ports

Port	Transferred
80	1.6 PB
443	354.0 TB
8080	194.2 TB
8081	2.5 TB
8082	1.8 TB
8083	1.3 TB
8084	1.1 TB

AS	AS	Transferred	Average Speed
AS1	AS2	224.5 TB	21.0952 gbps
AS1	AS2	96.6 TB	9.0790 gbps
AS1	AS2	96.2 TB	9.0369 gbps
AS1	AS2	69.1 TB	6.4974 gbps
AS1	AS2	69.1 TB	6.4953 gbps
AS1	AS2	50.8 TB	4.7780 gbps
AS1	AS2	50.5 TB	4.7437 gbps
AS1	AS2	48.3 TB	4.5426 gbps
AS1	AS2	48.2 TB	4.5314 gbps
AS1	AS2	39.0 TB	3.6654 gbps

AS	AS	Transferred	Average Speed
AS1	AS2	32.5 TB	3.0515 gbps
AS1	AS2	28.5 TB	2.6779 gbps
AS1	AS2	26.8 TB	2.5148 gbps
AS1	AS2	25.8 TB	2.4212 gbps
AS1	AS2	23.8 TB	2.2397 gbps
AS1	AS2	23.0 TB	2.1581 gbps

[see all...](#)

Top Source AS → Destination AS pairs, other vlans

Src AS	Dst AS	Transferred	Average Speed
AS1	AS2	65.0 TB	6.1084 gbps
AS1	AS2	39.2 TB	3.6810 gbps
AS1	AS2	32.9 TB	3.0917 gbps
AS1	AS2	32.5 TB	3.0559 gbps
AS1	AS2	20.3 TB	1.9105 gbps
AS1	AS2	20.0 TB	1.8771 gbps
AS1	AS2	17.8 TB	1.6685 gbps

Dashboard – First page important data in descending order

Total traffic in Gbps, Monthly



Top Vlans

Vlan ID	Name	Transferred
100	100	34.6 PB
101	101	5.2 PB
102	102	3.1 PB
103	103	2.8 PB
104	104	2.1 PB

Interfaces table

Agent ID/ iface	Interface name	Transferred	Average Speed
10000	10000	7.0 PB	24.3680 gbps
10000	10000	7.0 PB	24.3339 gbps
10000	10000	4.6 PB	15.8759 gbps
10000	10000	4.5 PB	15.7478 gbps
10000	10000	2.4 PB	8.4670 gbps

Top Source AS – Destination AS pairs, vlan 304

Src AS	Dst AS	Transferred	Average Speed
10000	10000	4.3 PB	14.8770 gbps
10000	10000	2.4 PB	8.4453 gbps
10000	10000	1.3 PB	4.6054 gbps
10000	10000	1.2 PB	4.1647 gbps
10000	10000	912.1 TB	3.0867 gbps

Example: monthly view

Options: Hour, Day, Week, Month, Year

Total traffic in Gbps for: **XXXXXXXXXX** & period: Daily



Top Vlans

Vlan ID	Name	Transferred
XXXXXX	XXXXXXXXXX	199.2 TB
XXXXXX	XXXXXXXXXX	154.1 TB

Top Source AS

Src AS	Transferred	Average Speed
XXXXXX	41.3 TB	3.8853 gbps
XXXXXX	2.3 TB	0.2204 gbps

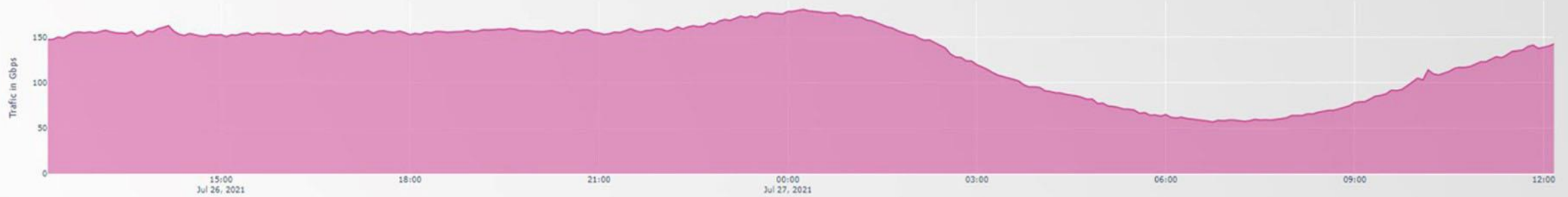
Top Destination AS

Dst AS	Transferred	Average Speed
XXXXXX	101.7 TB	9.5619 gbps
XXXXXX	59.9 TB	5.6280 gbps

Example: view of specific partner/customer traffic characteristics

Options: Quick links for special partners/customers in navigation bar

Traffic in Gbps for vlan: [redacted] & period: Daily



Top TCP Ports for [redacted]

Port	Transferred
[redacted]	1.0 PB
[redacted]	234.9 TB
[redacted]	113.3 TB
[redacted]	1.7 TB
[redacted]	1.5 TB
[redacted]	987.2 GB
[redacted]	840.4 GB

Top Source AS – Destination AS pairs for [redacted]

Src AS	Dst AS	Transferred	Average Speed
[redacted]	[redacted]	268.2 TB	25.2027 gbps
[redacted]	[redacted]	92.4 TB	8.6846 gbps
[redacted]	[redacted]	55.3 TB	5.1957 gbps
[redacted]	[redacted]	53.5 TB	5.0261 gbps
[redacted]	[redacted]	32.6 TB	3.0595 gbps
[redacted]	[redacted]	31.4 TB	2.9468 gbps
[redacted]	[redacted]	29.9 TB	2.8068 gbps

Example: view for specific VLAN

Options: Deeper analysis are achieved through single click on the parameter that you want to analyze.

Graph - [redacted]-100G, Daily



Top Vlans

Vlan ID	Name	Transferred
[redacted]	[redacted]	223.0 TB

[see all...](#)

Top mac src addr

MAC Address	Peer	Transferred	Average Speed
[redacted]	[redacted]	223.0 TB	20.9534 gbps

[see all...](#)

Top mac dst addr

Top Source AS -- Destination AS pairs, vlan [redacted]

Src AS	Dst AS	Transferred	Average Speed
[redacted]	[redacted]	133.9 TB	12.5869 gbps
[redacted]	[redacted]	26.9 TB	2.5289 gbps
[redacted]	[redacted]	8.1 TB	0.7641 gbps
[redacted]	[redacted]	6.1 TB	0.5754 gbps
[redacted]	[redacted]	5.2 TB	0.4909 gbps
[redacted]	[redacted]	4.2 TB	0.3966 gbps

Example: predefined query

Possibility to drill-down of traffic characteristics per every individual interface sorted in descending order

agent== and iface== from: 07/26/2021 11:39 AM to: 07/27/2021 11:39 AM filter

Dodaj upit

Filter traffic on: agent, iface, vlan, mac.src, mac.dst, as.src, as.dst
eg.: mac.dst=ff:ff:ff:ff:ff:ff and agent== and (iface== or iface==)

Stats for filter on traffic: agent== and iface==



Top SRC ASes

Source AS	Average speed
	19.6332 gbps
	0.5203 gbps
	0.1547 gbps
	0.1390 gbps
	0.1023 gbps
	0.0584 gbps
	0.0169 gbps
	0.0060 gbps

Top DST ASes

DST AS	Average speed
	12.9684 gbps
	2.5052 gbps
	0.7947 gbps
	0.6005 gbps
	0.4982 gbps
	0.4033 gbps
	0.3782 gbps
	0.3036 gbps

Top Source AS — Destination AS pairs

Src AS	Dst AS	Average Speed
		12.4602 gbps
		2.4219 gbps
		0.7594 gbps
		0.5605 gbps
		0.4896 gbps
		0.3948 gbps
		0.3610 gbps
		0.2941 gbps

Top mac src addr

MAC Address	Peer	Average Speed
		20.6566 gbps

Top mac dst addr

MAC Address	Peer	Average Speed
		18.5356 gbps
		0.6005 gbps
		0.4982 gbps
		0.3036 gbps

Custom filter

- ❑ custom combination of predefined parameter.
- ❑ possibility to save your own query

Site administration

AUTHENTICATION AND AUTHORIZATION

Groups	+ Add	Change
Users	+ Add	Change

SOX

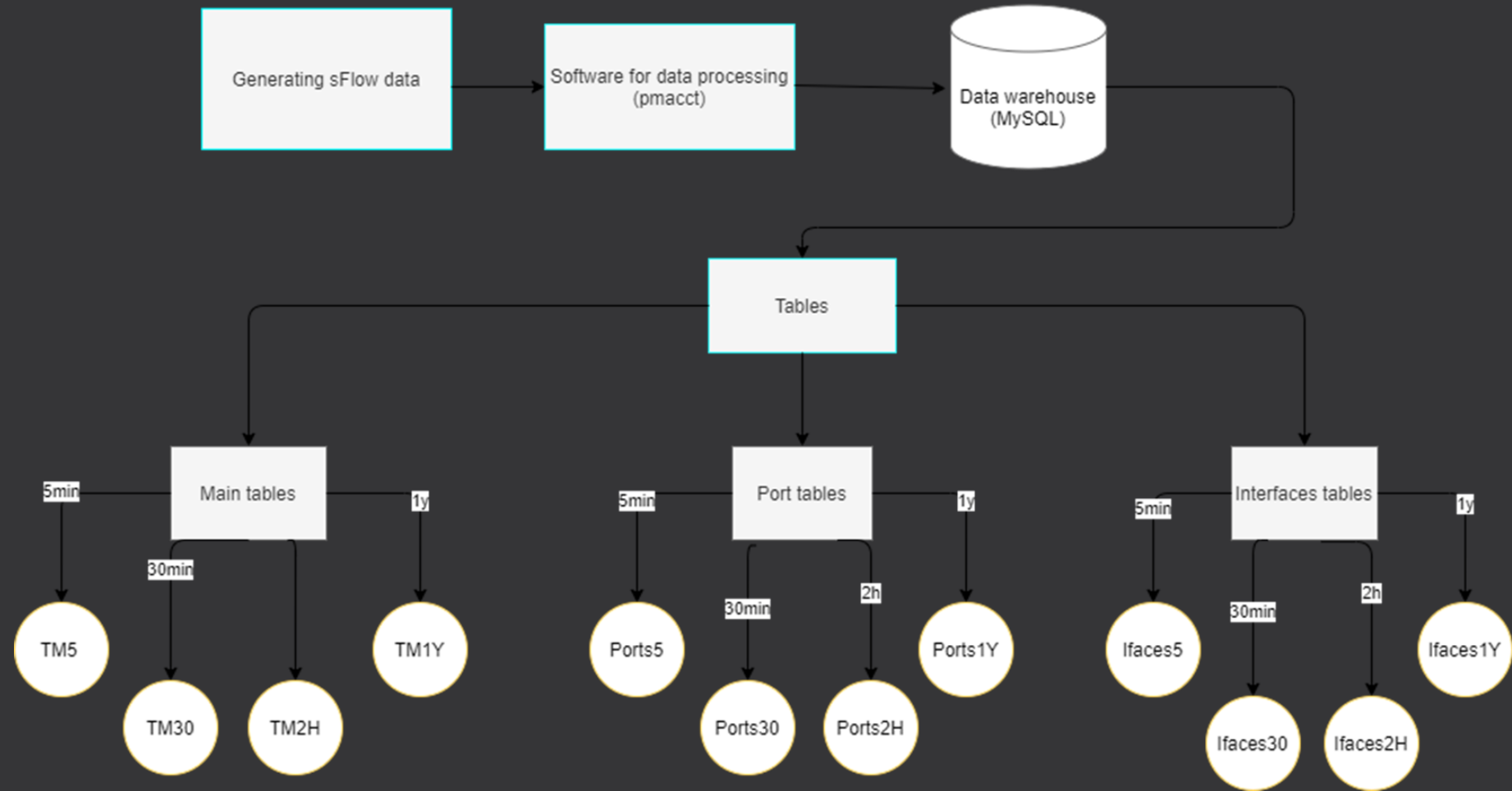
Asnss	+ Add	Change
Interfaceshows	+ Add	Change
Interfaccs	+ Add	Change
Peerss	+ Add	Change
Querless	+ Add	Change
Sox querless	+ Add	Change
Subnetss	+ Add	Change
Vlans	+ Add	Change

Recent actions

My actions

- Viewed...
- Created...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...
- Updated...
- Added...
- Changed...
- Deleted...

Admin panel: managing Users, sFlow data, ASNs, Peers, Interfaces, Subnets, VLANs



Uses pmaect as sflow collector (open-source software developed by Paolo Lucente)

Thank You!

Developico & SOX

Special Thanks to:

Paolo Lucente, Author of pmacct software

dr Nenad Krajnovic, Founder and CTO SOX

Zoran Perovic, Founder and CEO SOX