Mastering ntopng Flow Aggregation and Traffic Rules

Nicolo' Maio maio@ntop.org



Sept, 21-22 · Pisa

Main Issues to Tackle

- 1. Monitor selected SNMP devices, hosts, network interfaces, host pools, and networks.
- 2. Easily gather statistics about the traffic generated by a specific application protocol or a couple of client-server pairs.



Presentation Outline

- SNMP Devices Rules
- Host/Net Interface/Host Pool/Network
 Rules
- Exercise of Network Interfaces Rules
- Aggregated Live Flows
- Examples of Aggregated Live Flows in ntopng



SNMP Devices Rules [1/7]

• Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on

IP networks and for modifying that information to

change device behaviour.



SNMP Devices Rules [2/7]

SNMP Devices | 🛖 Interfaces Rules 🐴 🥰 🕰

Show 10 \sim entries Device Filter -C O ▼ Search: **SNMP Time Since** Last Poll Interfaces With Errors Actions **Device IP** Version Chart Description Last Poll Duration **Device Name** 192.168.2.1 v1 EdgeRouter-X-5-Port office router 2 00:41 00:01 ≣▪ 00:02 192.168.2.83 v1 vsphere-idrac 1 00:41 ≣▪ ≣▪ 192.168.2.106 MikroTik Ax3 RouterOS C53UiG+5HPaxD2H... 00:41 00:03 v1 ≣▪ 192.168.2.120 idrac-8YQXT72 00:41 00:02 v1 1 192.168.2.134 v2c devele Linux devele 6.2.0-26-ge... 00:41 00:01 ≣▼ 1 nTopSwitch 28-Port Gigabit Managed ... 192.168.2.167 v2c 1 00:41 00:08 ≣∙ 192.168.2.169 v1 **ProCurve Switch** ProCurve J9019B Switch 2... 1 00:41 00:04 ≣▪ 2510B-24 3Com Baseline 3Com Baseline Switch 292... 192.168.2.175 v1 00:41 00:04 ≣▪ Switch





←

SNMP Devices Rules [3/7]

Monitoring and discovering that a specific SNMP
 Device has exceeded traffic thresholds is not
 possible using the previously engaged alerts (such as Ingress Traffic, Egress Traffic, etc...)



SNMP Devices Rules [4/7]

With the SNMP Devices Rules, it is possible to monitor a specific SNMP device or a specific interface of a specific SNMP device with interval frequency checks of 5 minutes, 1 hour or 1 day.



SNMP Devices Rules [5/7]

- The Threshold Rule can be an upper or lower bound of Bytes, Packets or Interface Errors.
- •When a threshold is crossed ntopng will trigger an alert.

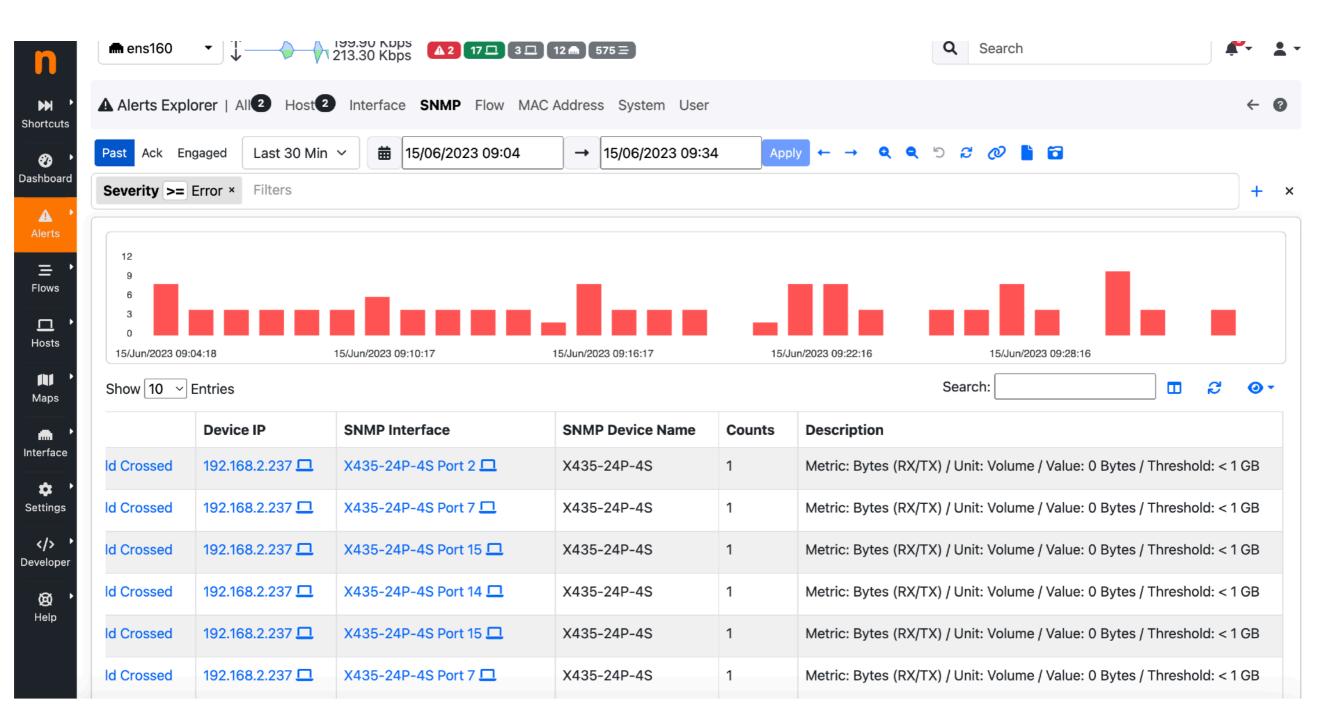


SNMP Devices Rules [6/7]

Select the SNMP device	► Shortcuts	Add Rule		×	* -	1
Select the SNMP device por	rt Alerts	Rule type Device	SNMP Device 3Com Baseline Switch (192.168.2.175)			÷
Select the metric	⊢ Sh Flows Hosts	Interface Metric	GigabitEthernet1/0/10 (10) ~ Bytes (RX/TX) ~			
Select the check frequency	Maps X	Check Frequency Threshold	5 Minutes ~ Volume ~ KB MB GB > < 1		Actio	
Select the rule threshold	Settings Constructions	 Interface: se Metric: select Frequency: Threshold: se upperbound Percentage frequency 5 	ect the SNMP Device to be analyzed elect the interface of the SNMP device that needs to be analyzed. act the metric to be analyzed (e.g. errors -> the SNMP metric errors) select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes) select the type of threshold (Volume, Throughput or Percentage), lowerbound or d, and the threshold that, if exceeded, is going to trigger an alert Threshold: is calculcated beetwen the last two frequency checks (e.g. <1% with 5 Min -> if the difference between precedent frequency and the last 5 minutes chec n 1% trigger and alert)		> emove	>>



SNMP Devices Rules [7/7]





Host/Interface/HostPool/Network Rules [1/4]

- Same as SNMP Rules but for hosts, network interfaces, host pool and network.
- In this case is possible to active monitor a specific host, or a specific network interface or a specific host pool or a specific network with interval frequency checks of 5 minutes, 1 hour or 1 day.



Host/Interface/HostPool/Network Rules [2/4]

In case of Rule Type Host	Add Rule		×
indicate the Host, Otherwise select an Interface or	Rule type	Host Interface Host Pools Networks	
Select an Host Pool or Select a Local Network	Target	A local host IP or '*' for checking all local hosts	
	Metric	Traffic	~
Select the metric	Check Frequency	5 Minutes	~
Select the check frequency	Threshold	Volume ~ KB MB GB > < 1	
Select the rule threshold	 analyzed) or Metric: select Frequency: Threshold: select upperbound Percentage frequency 5 	rt the IP of a Local Host to be analyzed or a * (meaning that all Local Hosts has to r select a local network interface ct the metric to be analyzed (e.g. DNS -> the DNS traffic) select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes) select the type of threshold (Volume, Throughput or Percentage), lowerbound or d, and the threshold that, if exceeded, is going to trigger an alert Threshold: is calculcated beetwen the last two frequency checks (e.g. <1% with 6 Min -> if the difference between precedent frequency and the last 5 minutes che n 1% trigger and alert)	



Host/Interface/HostPool/Network Rules [3/4]

Metrics for the Host and Network Interface Rules:

- Traffic RX / TX (or both),
- Score
- Application Traffic.

\cdot Metrics for the HostPools Rules:

- Traffic RX / TX (or both),
- Active Devices,
- Active Hosts,
- Blocked Flows

\cdot Metrics for the Network Rules:

- Broadcast Traffic RX / TX (or both)
- Traffic RX / TX (or both)
- Engaged Alerts
- Round Trip Time
- Score
- TCP Packets KeepAlive
- TCP Packets Lost
- •TCP Packets Out-Of-Order
- •TCP Retransmitted Packets



Host/Interface/HostPool/Network Rules [4/4]

men0 - ↓	37.10 Kbps 57.30 Kbps 1≡▲	13 ⊒ ▲ 24 □ 23 (1) □	10 📾 182 =	Q Se	arch			2 .	. •	In Actions menu the edit and
Local Traffic Rules										delete rule
Show 10 ~ entries					C	+ Search:				options are present
Target 🍦	Туре	Metric 🕴	Check Frequency	Last Measurement	•	Threshold	\$	Actions	s /	present
PippoPool	Host Pool 🗖	Active Devices	5 Minutes	0			> 15	≣▪		
192.168.1.0/24	Network 🗖	TCP Packets Lost	5 Minutes	0			> 100			
NOTES • Trigger an alert when a local • To add a new rule, click the • To remove a rule, click on th	'+' symbol on the right	side above the table (nex		remove		« <		> >		
ntopng Enterprise XL v.5.7.230606 (mad	cOS 13.4.1)		© 1998-23 - ntop			§ 15:12:52 +02	00 UTC U	Jptime: 30	:33	
					_					14



Exercise of Network Interfaces Rules



Sept, 21-22 · Pisa

Exercise of Network Interfaces Rules [1/1]

- •Set a Network Interface Rule with threshold > 1 KB
- Set a notification endpoint and recipient to receive a message on telegram when the Threshold is crossed.
- Restart ntopng
- •(The alert name is 'Network Interface Volume Exceeded')





Aggregated Live Flows [1/11]

To find the total traffic for a specific
 Application Protocol on the Live Flows
 page, a user needs to activate the protocol
 filter and sum the traffic bytes.



Aggregated Live Flows [2/11]

 With Aggregated Live Flows, it is easy to quickly discover the total traffic and various other information related to a specific Application Protocol.



Aggregated Live Flows [3/11]

- •The current aggregation criteria are:
 - Application Protocol
 - ∘Client
 - •Server
 - Client-Server
 - Client-Server-Destination Port
 - Client-Server-App.Proto
 - ∘Info



Aggregated Live Flows [4/11]

Clicking on the flows icon Is possible to jump to the live flows filtered by the specific row values of the aggregation criteria

Clicking on the link in the Client or Server Column is possible to jump to the Host details page

	📾 en0	 	23 □ 20 □ 11 ⋒ 172 Ξ		Q	Search		
Ξ	E Live	Flows 🏫 Analysis						
	Flow A	ggregation Key: Client / Server / Dst Port 🗸						
	Show	10 V Entries						2
		Client	Server	Flows	Tot. Score	Breakdown	Traffic Sent	т
	=	desktop-maio.homenet.telecomitalia.it 🚺 🚮 🕑 💻	224.0.0.251 M 🗔:0	1		Sent	46 Bytes	;
	=	192.168.2.11 🖪 🖻 🗖	239.255.255.250 M 💻:0	1		Sent	46 Bytes	
	=	host-004.homenet.telecomitalia.it 💶 🚠 🕑 🗖	224.0.0.251 M 💻:5353	1		Sent	79 Bytes	
	=	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 🗖	224.0.0.251 M 🗔:5353	1		Sent	87 Bytes	;
	=	fe80::101b:a729:c77d:e881 💶 P 🗖	ff02::fb M 🗔:5353	1		Sent	99 Bytes	:
	=	macbook-pro-di-nicolo.local 💶 P 🗔	ff02::fb M 🗔:5353	1		Sent	107 Bytes	:
	=	mbp-di-nicolo.homenet.telecomitalia.it 🕕 🚓 🕑 📮	17.57.146.173 R 🗔:5223	1	50	Sent Rcvd	166 Bytes	
	=	mbp-di-nicolo.homenet.telecomitalia.it 🚺 🛻 🕑 💻	h388x.homenet.telecomitalia.it 🕒 🚠 P 🗔:0	3		Sent	210 Bytes	
	=	samsung.homenet.telecomitalia.it 📭 🛻 🕑 💻	224.0.0.251 M 🗔:5353	1		Sent	248 Bytes	
	Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 🕑 💻	h388x.homenet.telecomitalia.it 🔲 🚠 🖻 🗔:53	8	10	Sent Rcvd	690 Bytes	



Aggregated Live Flows [5/11]

Application Protocol Criteria

ve Flows	Analysis								•
v Aggregatio	on Key: Application Protocol	~							
w 10 🗸 En	tries					S	earch:		8 🔍 💁
Appli	cation Protocol 🔹	Flows	Tot. Score	Clients	Servers	Breakdown	Traffic Sent	Traffic Rcvd	Total Traffic
= WireG	Guard Guess	1	10	1	1	Sent Rcv	57.35 KB	10.88 KB	68.24 KB
= ? Unk		1		1	1	Sent	545.69 KB	0 Bytes	545.69 KE
TLS.V	imeo DPI	1		1	1	Sent Rcvd	2.06 KB	5.29 KB	7.35 KB
	S.Spotify DPI	5		1	2	Rcvd	76.96 KB	13.19 MB	13.27 MB
TLS.G	Bithub DPI	1		1	1	Sent Rcvd	5.54 KB	5.83 KB	11.37 KB
TLS.D	Discord DPI	2	10	1	2	Sent Rcvd	272.84 KB	832.27 KB	1.08 MB
TLS	DPI	10	160	2	9	Sent Rcvd	511.39 KB	1.21 MB	1.71 MB
= SSDP	DPI	90	10	4	2	Sent B	68.32 KB	3.83 KB	72.15 KE
= Sp	otify DPI	1		1	1	Sent	32.92 KB	0 Bytes	32.92 KE
= G+ QI	JIC.GoogleServices	1		1	1	Sent Rcvd	2.6 KB	3.04 KB	5.65 KE



Aggregated Live Flows [6/11]

Client Criteria

en0 ▼ ↓ ↓ 7.30 Kbps 1=▲ 2=▲ 21□ 2	2 🗆 8 🍙	129 ☰			Q Search		₽ , 2
Live Flows 🏫 Analysis							€
ow Aggregation Key: Client ~							
ow 10 ~ Entries							; 💽 0-
Client	Flows	Tot. Score	Servers	Breakdown	Traffic Sent	Traffic Rcvd	Total Traffic
= 149.154.167.43 R 🗖	1	10	1	Sent Rcvd	264 Bytes	120 Bytes	384 Bytes
= 192.168.1.28 🛯 🚓 🖻 🖵	1	10	1	Sent	868 Bytes	0 Bytes	868 Bytes
= host-003.homenet.telecomitalia.it 🔳 🚠 🖻 🗖	86		1	Sent	62.21 KB	0 Bytes	62.21 KE
= fe80::ec26:71ff:fe98:5e19 🚺 🕑 🗖	1		1	Sent	94.91 KB	0 Bytes	94.91 KE
= 192.168.2.11 R P 🗖	2		2	Sent	550.1 KB	0 Bytes	550.1 KE
mbp-di-nicolo.homenet.telecomitalia.it 🔳 🚠 🖻 🗖	47	270	25	S Rcvd	992.52 KB	15.3 MB	16.27 ME
Showing page 1 of 1: total 6 rows							< 1 >



Aggregated Live Flows [7/11]

Client / Server Criteria

📠 en0	• • ↓ • • • • • • • • • • • • • • • • •	21□ 22□ 8 ⋒ 129 Ξ		٩	Search		Å .	, 1
∃ Live	Flows 🏫 Analysis							÷
Flow A	ggregation Key: Client / Server 🗸 🗸							
Show	10 V Entries						2 🔍 🤇	0 •
	Client	Server	Flows	Tot. Score	Breakdown	Traffic Sent	Traffic Rcvd	Tota
=	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 믿 💻	224.0.0.251 M 🗖	1		Sent	396 Bytes	0 Bytes	3
=	macbook-pro-di-nicolo.local 🚺 P 🎞	ff02::fb M 🗖	1		Sent	456 Bytes	0 Bytes	4
Ξ	peppeasusi7.homenet.telecomitalia.it 🚺 🚠 P 🗖	239.255.255.250 м 🗖	1	10	Sent	868 Bytes	0 Bytes	8
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	host-003.homenet.telecomitalia.it 📘 🚠 P 💻	2		<mark>Sen</mark> Rcvd	1.39 KB	3.83 KB	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	239.255.255.250 M 🗖	2		Sent	1.68 KB	0 Bytes	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	162.159.138.60 R 🗖	1		Sent Rcvd	2.06 KB	5.29 KB	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 🚺 🚠 P 💻	h388x.homenet.telecomitalia.it 🔲 🛻 P 💻	27	10	Sent Rcvd	2.16 KB	3.61 KB	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	216.58.209.35 R 🗖	1		Sent Rcvd	2.34 KB	3.26 KB	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	142.250.180.138 R 🗖	1		Sent Rcvd	2.6 KB	3.04 KB	
Ξ	mbp-di-nicolo.homenet.telecomitalia.it 💶 🚠 P 💻	3.73.173.154 R 🗖	1		S Rcvd	2.83 KB	24.61 KB	:
Show	ing page 1 of 4: total 31 rows					< 1	2 3 4	>



Aggregated Live Flows [8/11]

Client / Server / App. Proto

en0	21□ 9 ⋒ 129 Ξ	Q Search	h
Live Flows 🏫 Analysis			
ow Aggregation Key: Client / Server / App. Proto 🗸			
now 10 ~ Entries		Search:	
Client	Server	Application Protocol	Flows
= 192.168.1.47 🔳 🚠 🕑 💻	224.0.0.251 M 🗖	IGMP Guess	1
= 192.168.2.11 R P 🗖	239.255.255.250 м 🗖	IGMP Guess	1
mbp-di-nicolo.homenet.telecomitalia.it 🛯 🚠 Р 🖵	h388x.homenet.telecomitalia.it 🛯 🛻 P 🗖	DNS.ntop DPI	2
mbp-di-nicolo.homenet.telecomitalia.it 🛯 🚓 P 🖵	h388x.homenet.telecomitalia.it 💶 🛻 P 💻	G+ DNS.GoogleDocs DPI	2
mbp-di-nicolo.homenet.telecomitalia.it 🛯 🚠 P 🖵	h388x.homenet.telecomitalia.it 🛯 🛻 P 🗖	CNS.AppleiTunes	2
mbp-di-nicolo.homenet.telecomitalia.it 🚺 🚠 P 🖵	h388x.homenet.telecomitalia.it 💶 👬 P 🗖	G+ DNS.GoogleServices DPI	2
mbp-di-nicolo.homenet.telecomitalia.it 🚺 🚠 P 🖵	h388x.homenet.telecomitalia.it 🚺 🛻 P 🗖	CONS.Apple DPI	3
mbp-di-nicolo.homenet.telecomitalia.it 🚺 🚠 P 🖵	h388x.homenet.telecomitalia.it 🚺 🛻 P 🗖	G+ DNS.Google DPI	4
mbp-di-nicolo.homenet.telecomitalia.it 🚺 🚠 P 🖵	h388x.homenet.telecomitalia.it 🚺 🛻 P 🗖	DNS.Discord DPI	4
mbp-di-nicolo.homenet.telecomitalia.it 🔲 🚠 🕑 🖵	224.0.0.251 M 🗖		1



<

Aggregated Live Flows [9/11]

Client / Server / Dst. Port

E Live Flows 🏫 Analysis						
						÷
Flow Aggregation Key: Client / Server / Dst Port 🗸						
Show 10 V Entries					ຊ 💽 🤇	0 -
Client Server	Flows	Tot. Score	Breakdown	Traffic Sent	Traffic Rcvd	Tot
■ 192.168.2.11 R P □ 239.255.255.250 M □:0	1		Sent	46 Bytes	0 Bytes	
desktop-maio.homenet.telecomitalia.it 🔳 🚓 🕑 🗖 224.0.0.251 M 🗔:0	1		Sent	46 Bytes	0 Bytes	
host-001.homenet.telecomitalia.it 🔳 🚓 Р 💷 224.0.0.251 M 🗔:5353	1		Sent	78 Bytes	0 Bytes	
mbp-di-nicolo.homenet.telecomitalia.it L 🛔 P 🗔 h388x.homenet.telecomitalia.it L 🛔 P 🗔:0	4		Sent	280 Bytes	0 Bytes	2
mbp-di-nicolo.homenet.telecomitalia.it L the P I 224.0.0.251 M I:5353	1	10	Sent	396 Bytes	0 Bytes	3
macbook-pro-di-nicolo.local L P L ff02::fb M 1:5353	1	10	Sent	456 Bytes	0 Bytes	4
mbp-di-nicolo.homenet.telecomitalia.it L 🚠 P 🗖 23.41.187.83 R 🗔:443	1		<mark>Se</mark> Rcvd	1.63 KB	7.96 KB	
mbp-di-nicolo.homenet.telecomitalia.it L . P . h388x.homenet.telecomitalia.it L . P . :53	21	30	Sent Rcvd	1.71 KB	3.49 KB	
mbp-di-nicolo.homenet.telecomitalia.it L 🚓 P 🗖 142.250.180.164 R 🗔:443	1		Sent Rcvd	1.71 KB	2.51 KB	
mbp-di-nicolo.homenet.telecomitalia.it L 🚓 P 🗔 162.159.138.60 R 🗔:443	1		Sent Rcvd	2.11 KB	5.35 KB	



Aggregated Live Flows [10/11]

Info Criteria 8.70 Kbps 38.00 Kbps Q Search 📾 en0 • 2 🗕 🗛 🚺 22 🖵 👖 23 🖵 👖 9 🧰 🕺 141 🚍 🤇 ∃ Live Flows | **↑** Analysis ← \sim Flow Aggregation Key: Info Show 10 ~ Entries Search: C 0. Info Flows Tot. Score Clients Servers Breakdown Traffic Sent Traffic Rcvd **Total Traffic** _eerogw._tcp.local 1 1 1 78 Bytes 0 Bytes 78 Bytes Ξ Sent Rcvd 28.1.168.192.in-addr.arpa 1 10 1 1 85 Bytes 135 Bytes 220 Bytes Ξ Sent Rcvd 47.1.168.192.in-addr.arpa 1 10 1 1 85 Bytes 136 Bytes 221 Bytes Ξ Sen Rcvd smoot-searchv2-aeuc1b.v.aaplimg.com 1 1 1 95 Bytes 310 Bytes 405 Bytes Ξ 2 Sent Rcvd 1 389 Bytes www.ntop.org 1 144 Bytes 245 Bytes Ξ Sent Rcvd e673.dsce9.akamaiedge.net 2 1 1 170 Bytes 401 Bytes 571 Bytes Ξ Sent Rcvd 2 gs-loc.ls-apple.com.akadns.net 1 1 180 Bytes 434 Bytes 614 Bytes Ξ Sent Rcvd 2 stocks-data-service.lb-apple.com.akadns.net 1 206 Bytes 483 Bytes 689 Bytes 1 Ξ 2 20 2 2 9.1.e.5.8.9.e.f.f.f.1.7.6.2.c.e.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa 1.02 KB 1.02 KB 0 Bytes Ξ Rcvd stocks-data-service.apple.com 1 1 1 1.63 KB 7.96 KB 9.59 KB Ξ Showing page 1 of 3: total 22 rows 3 > 2 <



Aggregated Live Flows [11/11]

Server Criteria

en0 ▼ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	23 🗆 9 🏛 142	3			Q Search		₽ .
ve Flows 🏫 Analysis							
v Aggregation Key: Server ~							
w 10 v Entries							c 💿 o
Server	Flows	Tot. Score	Clients	Breakdown	Traffic Sent	Traffic Rcvd	Total Traffic
= ff02::fb M □	1	10	1	Sent	563 Bytes	0 Bytes	563 Byt
= 224.0.0.251 M □	3	10	3	Sent	607 Bytes	0 Bytes	607 Byt
host-003.homenet.telecomitalia.it 🚺 🛻 🕑 🗖	1		1	Sent	714 Bytes	0 Bytes	714 By
149.154.167.43 R 🖵	1		1	S Rcvd	928 Bytes	12.93 KB	13.83
= 17.57.172.11 R 🗖	1		1	Sent Rcvd	1009 Bytes	3.13 KB	4.12
= 23.41.187.83 R 🗖	1		1	<mark>Ser</mark> Rcvd	1.63 KB	7.96 KB	9.59
= 142.250.180.164 R 🗖	1		1	Sent Rcvd	1.71 KB	2.51 KB	4.22
17.36.206.5 R	1		1	Sent Rcvd	1.81 KB	6.47 KB	8.28
h388x.homenet.telecomitalia.it 🕒 🚓 🕑 🗖	25	30	1	Sent Rcvd	2 KB	3.73 KB	5.73

1 2 3 >



Examples of Aggregated Live Flows in ntopng





https://github.com/ntop/ntopng



Sept, 21-22 · Pisa