

ntopng 2023: News & Updates

Matteo Biscosi
Nicolò Maio

What Changed

Main Focus/Changes:

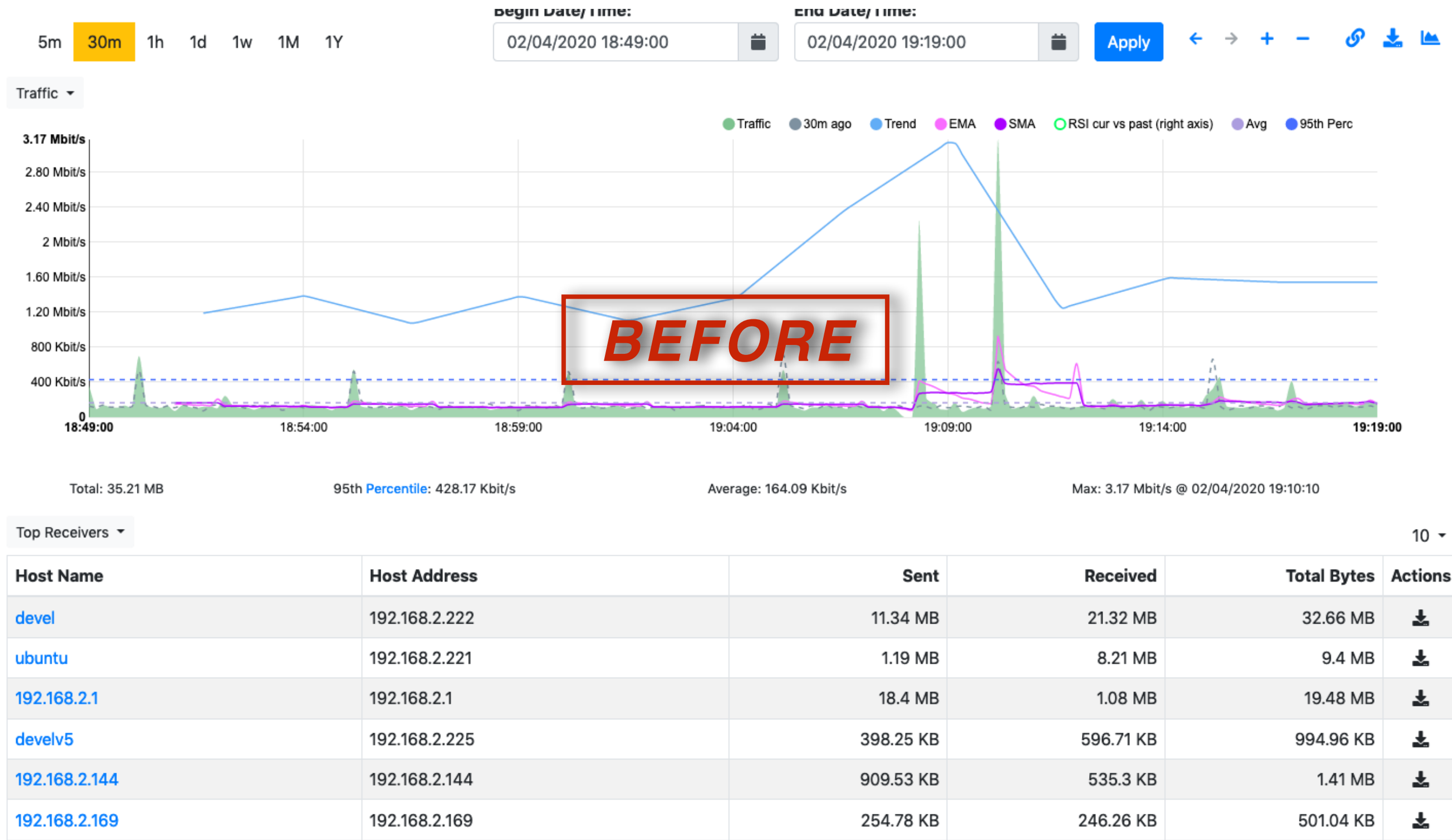
Last Year	Now
Alerts & Checks	Cybersecurity
Behavior Analysis	Traffic Analysis
Historical Flows (ClickHouse)	Historical Flows (Improvements)
Integrations	Integrations
	User Interface

New ntopng Model Available: Enterprise XL

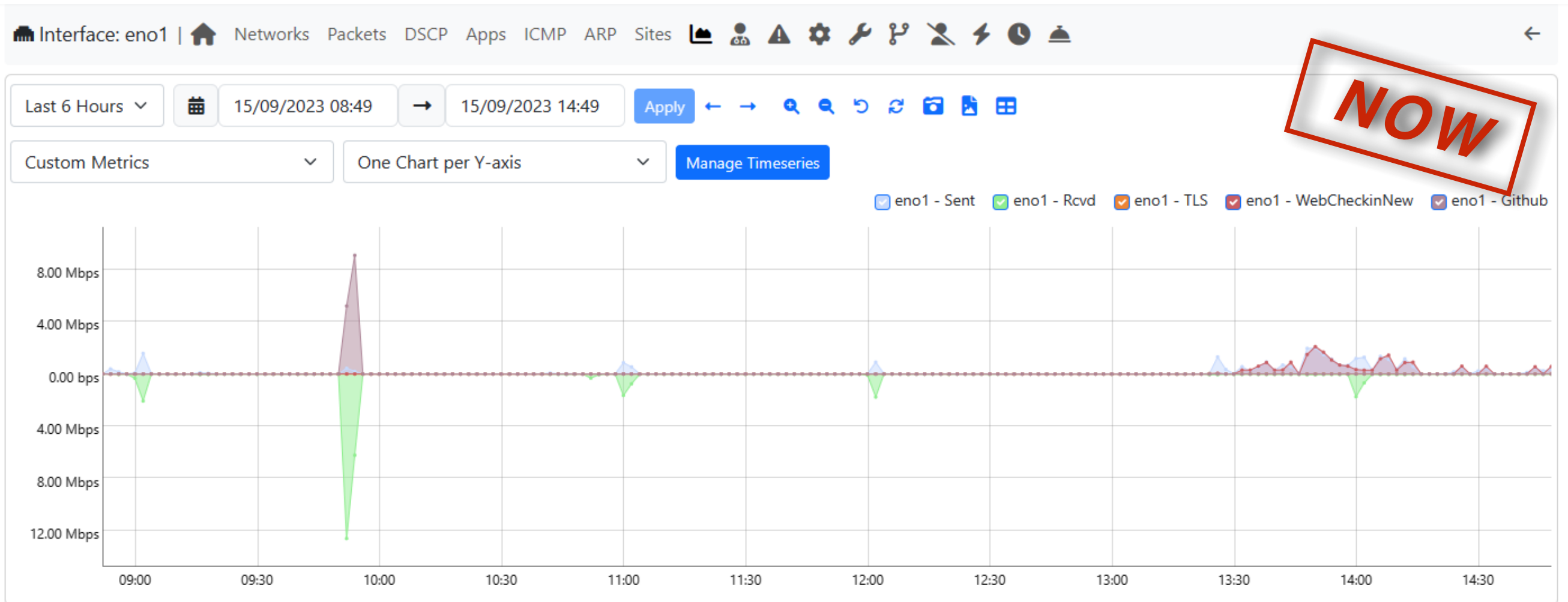
XL Model:

- Increased the maximum number of exporters (reaching 1024 total exporters)
- Increased the maximum number of monitored interfaces (up to 64)
- Support to Host Flow Sankey & other features...

User Interface Refactoring: Charts (1/2)



User Interface Refactoring: Charts (2/2)



Metric	Average	95th Percentile	Max	Min	Total
eno1 - Sent	164.31 Kbps	1.12 Mbps	1.98 Mbps	0.00 bps	420.75 MB
eno1 - Rcvd	170.33 Kbps	90.77 Kbps	12.60 Mbps	0.00 bps	436.15 MB
eno1 - TLS	5.83 Kbps	11.16 Kbps	31.49 Kbps	0.00 bps	14.94 MB
eno1 - WebCheckinNew	107.90 Kbps	684.34 Kbps	2.10 Mbps	0.00 bps	276.29 MB
eno1 - Github	79.92 Kbps	291.37 bps	9.09 Mbps	0.00 bps	204.64 MB

New Dashboard... (1/2)

1
Engaged Alerts



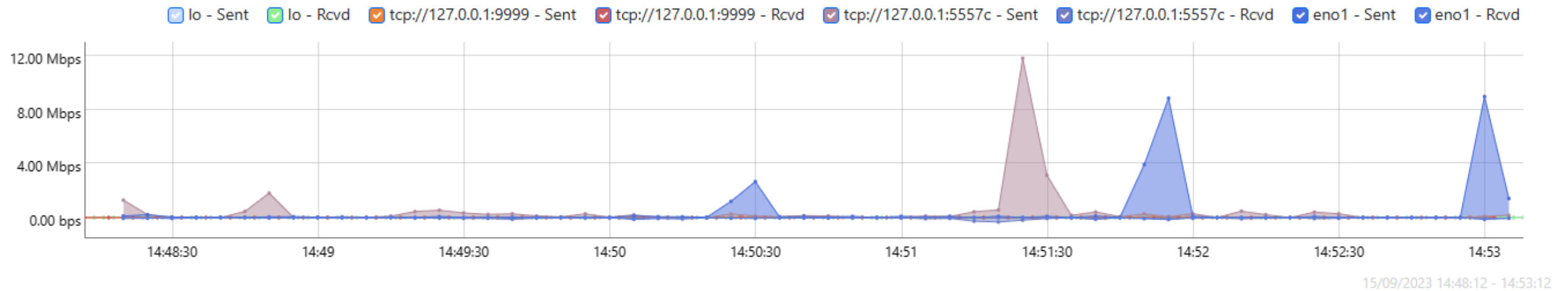
10
Active Hosts



58
Active Flows



Interfaces Traffic



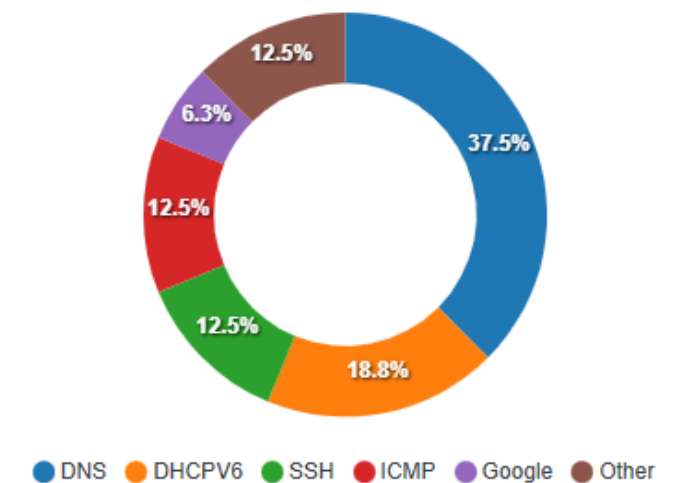
Top Local Hosts

Host	Current Traffic
devel	204.90 Kbps
192.168.2.153	189.90 Kbps
dns.google	522.50 bps
_gateway	240.00 bps

Top Remote Hosts

Host	Current Traffic
------	-----------------

Top Applications



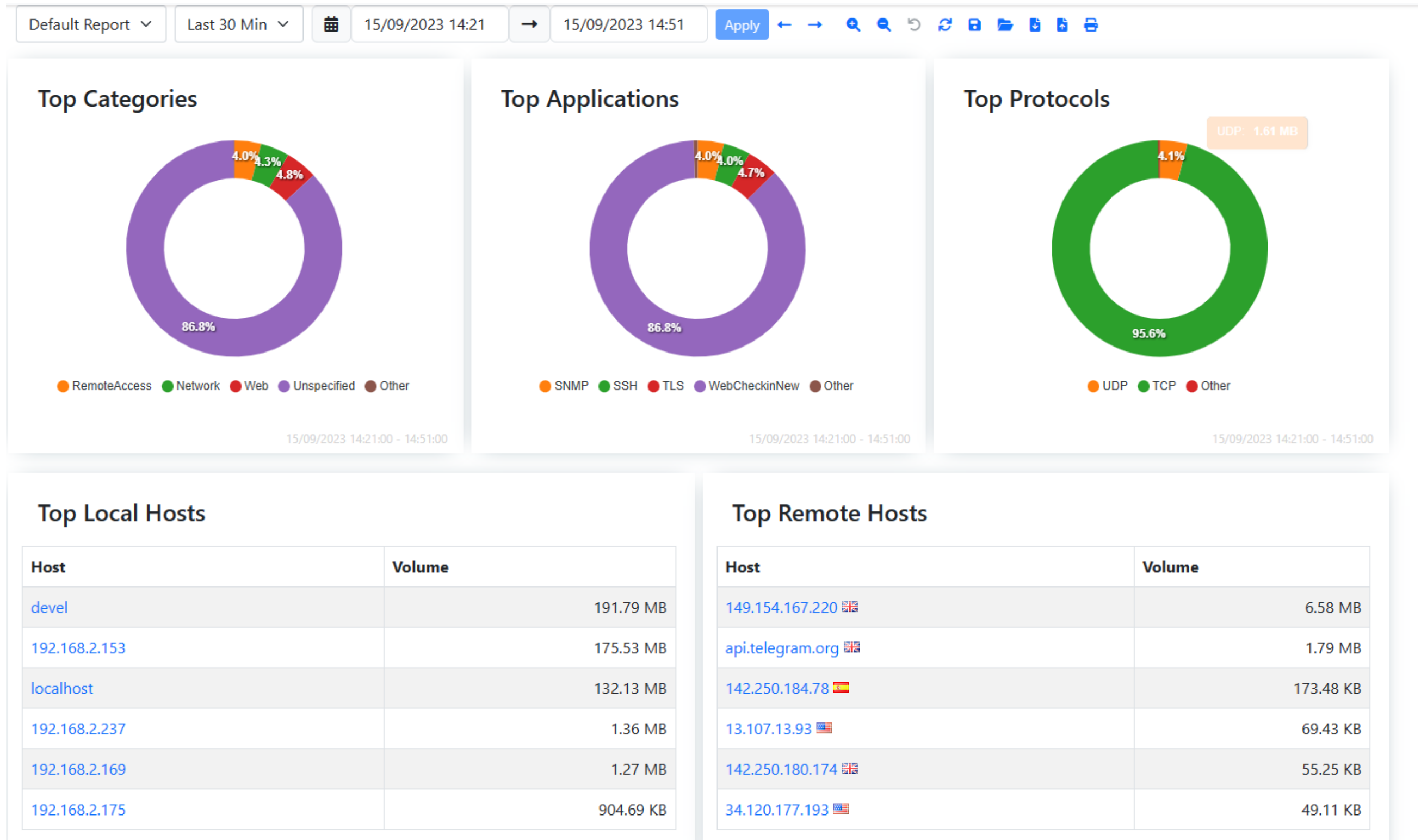
New Dashboard... (2/2)

A different Dashboard based on:

- Model (Pro, Enterprise M, ...)
- Configuration (ClickHouse enabled or not)

In the near future: ability to create custom dashboards from ntopng UI

...& Traffic Report (1/2)



...& Traffic Report (2/2)

Now it can:

- Be Printed / Uploaded / Downloaded
- Sent via E-Mail!
- Different Reports available
- A lot more in the future...

E-Mail Report

		MailReports	Email	EmailEndpoint	18:38:40	1	0	0 %
--	--	-------------	-------	---------------	----------	---	---	-----



New Report Available

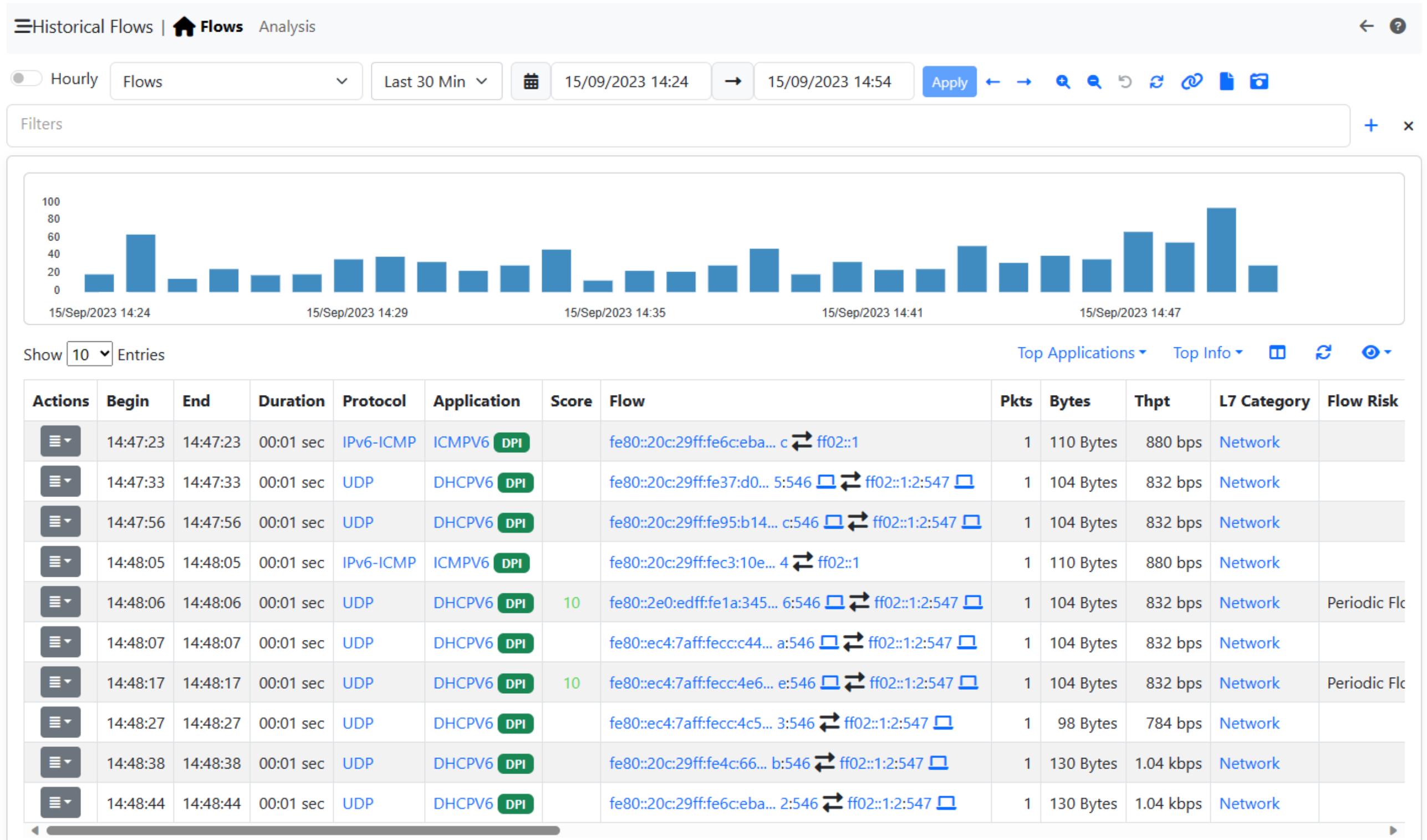
There is a new daily report auto-2023-Sep-15-1694728866 available in ntopng for interface <tcp://127.0.0.1:6666c> under the Reports section. A retention time of 30 days is configured in the ntopng Preferences, it is recommended to download and backup the report.

Check it out!

Go to Report

Historical Flows

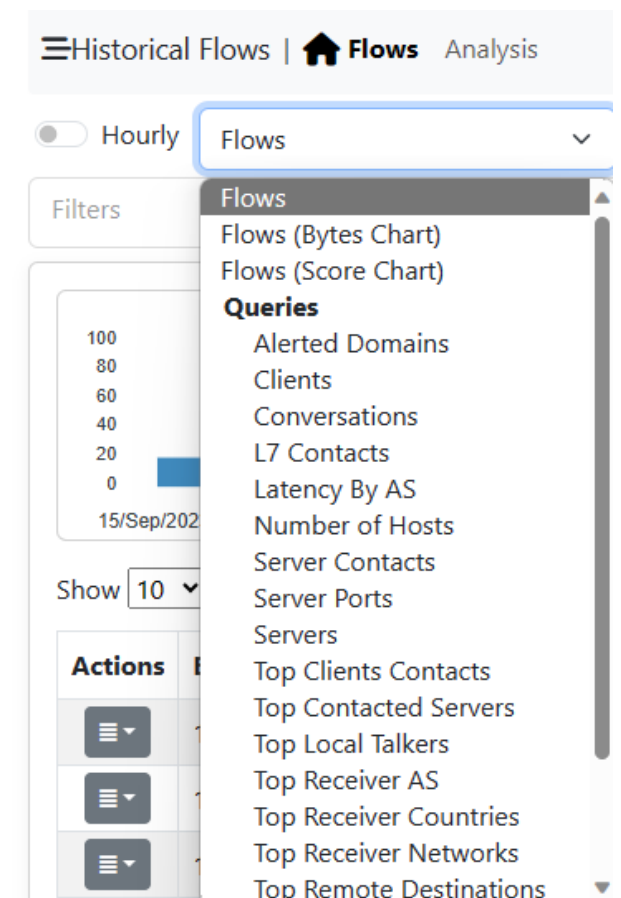
User Interface Refactoring... (1/2)



Historical Flows

User Interface Refactoring... (2/2)

- Changed tables:
 - More Flexible (resizable columns)
 - A lot more Fast
 - Configurable (choose which column to display)
- Added many new Presets (Queries):
 - Top Sender/Receiver Network
 - Top Sender/Receiver Country
 - ...



...Historical Flows Aggregation (1/3)...

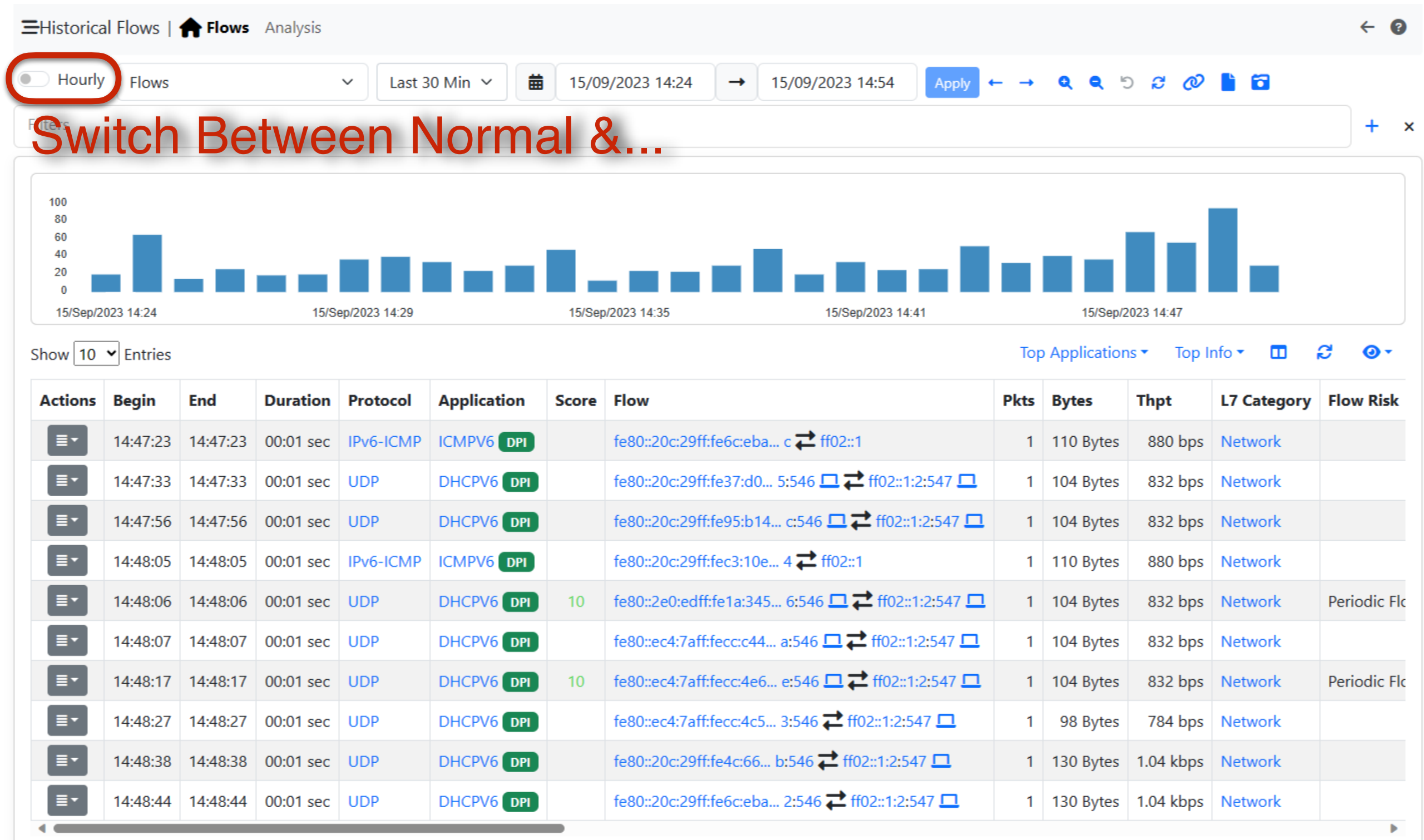
Have less information but more Data!

Keeping all last month Flows in the Database could cost a lot of disk

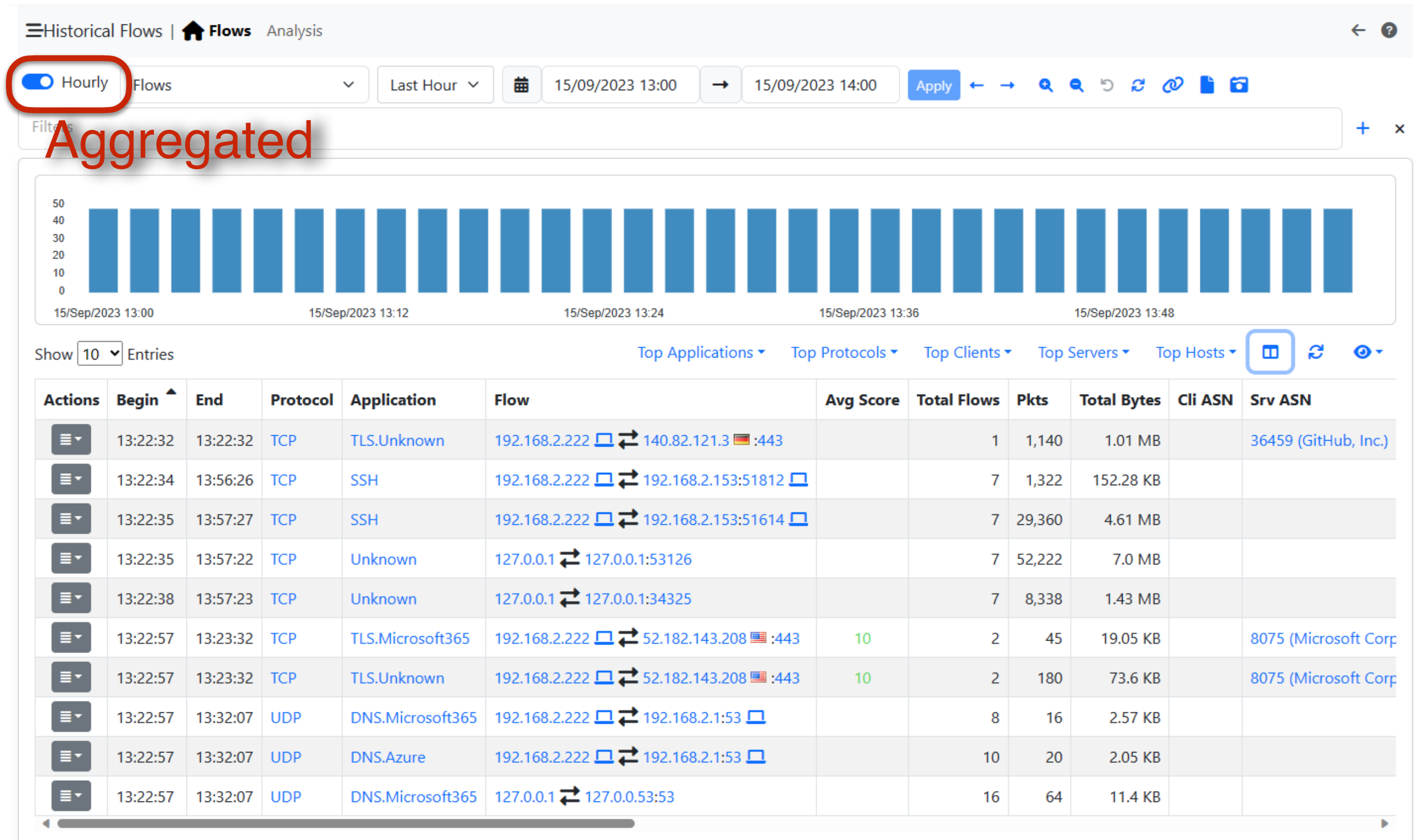


Just keep an aggregation of flows (compact similar flows in a single entry) in order to be able to keep more data

...Historical Flows Aggregation (2/3)...



...Historical Flows Aggregation (2/3)...



...Historical Flows Aggregation (3/3)...

99.6 GB vs 629.1 MB

- Flows Table Size: 99.6 GB —
- Hourly Flows Table Size: 629.1 MB —
- Alert Tables Size: 6.9 MB (Flow Alerts are included in the Flow Table Size) —

Database Table Records:

Flows: 2,526,547,711 [42 bytes/record]
Hourly Flows: 14,230,000 [46 bytes/record]
Alerts: 47,985,994

Compression of data:
2.5B vs 14.2M Flows

ClickHouse

ClickHouse Flows/Alerts Data Retention

Number of days to keep raw (unaggregated) flows (if enabled) and alerts. Default: 30 days.

15

ClickHouse Aggregated Flows Data Retention

Number of days to keep aggregated flows informations (it must be larger than unaggregated flows retention).
Default: 60 days.

60

15 days of data vs 60 days of data!

...Historical Flows Clustering

Export flows from multiple ntopng towards:

- A single/stand-alone ClickHouse instance
- a ClickHouse Cluster

A ClickHouse cluster can provide redundancy, capacity, and performance



... & more Traffic Analysis

Many new pages to analyze the traffic and to understand what's happening:



- Live Flows Aggregation
- Asset Map
- Ports Analysis
- Host Sankey
- Networks
- Inactive Local Hosts
- ...

































































































































































... & more Traffic Analysis

Live Flows | Analysis

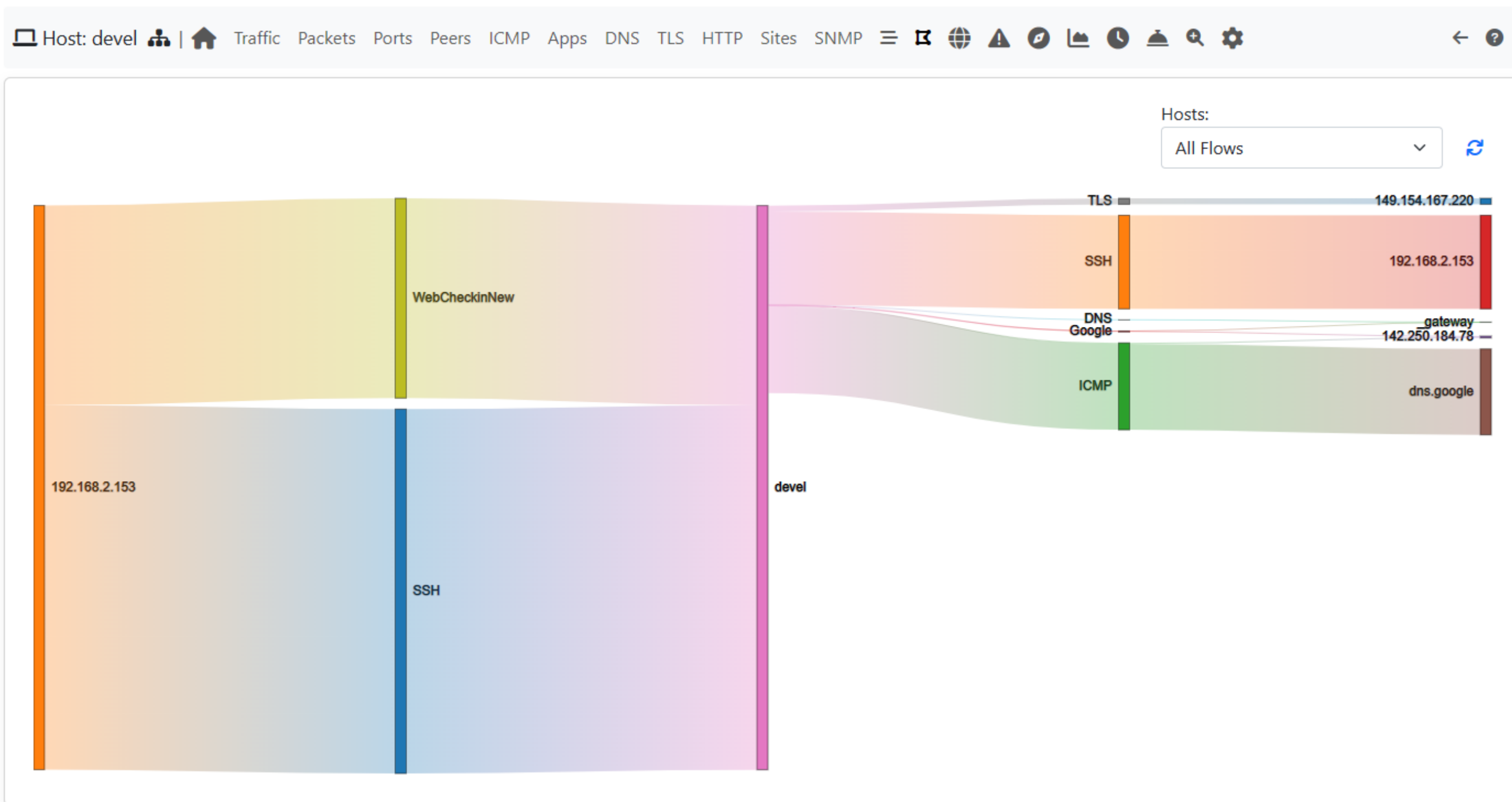
Flow Aggregation Key: Client / Server / App. Proto

Show 20 Entries

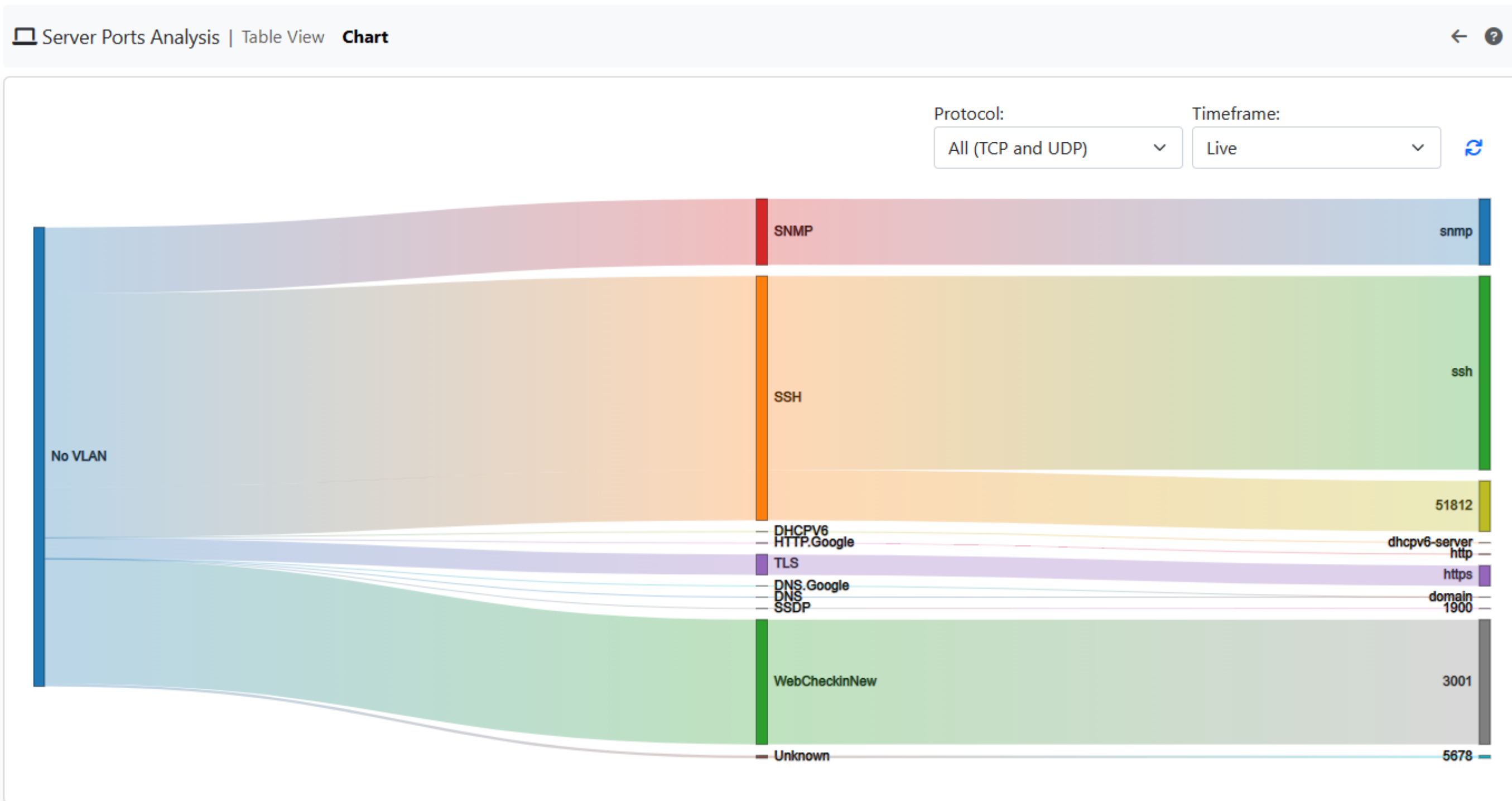
Search:    

	Client	Server	Application Protocol	Flows	Tot. Score	Clients	Servers	Breakdown	Traffic Sent	Traffic Rcvd
	192.168.2.153     	192.168.2.82    	HTTP 	1		1	1		60 Bytes	0 Byte
	192.168.2.153     	192.168.2.82    	TLS 	1		1	1		60 Bytes	0 Byte
	192.168.2.153     	192.168.2.82    	ICMP 	1		1	1		60 Bytes	0 Byte
	fe80::ec4:7aff:fecc:4c53    	ff02::1:2   	DHCPV6 	1		1	1		98 Bytes	0 Byte
	fe80::20c:29ff:fe37:d05    	ff02::1:2   	DHCPV6 	1		1	1		104 Bytes	0 Byte
	fe80::ec4:7aff:fecc:c44a    	ff02::1:2   	DHCPV6 	1	10	1	1		104 Bytes	0 Byte
	fe80::2e0:edff:fe1a:3456    ...	ff02::1:2   	DHCPV6 	1		1	1		104 Bytes	0 Byte
	fe80::20c:29ff:fe95:b14c    	ff02::1:2   	DHCPV6 	1		1	1		104 Bytes	0 Byte
	fe80::20c:29ff:fe4c:66b    	ff02::1:2   	DHCPV6 	1		1	1		130 Bytes	0 Byte
	192.168.2.198     	224.0.0.251   	MDNS 	1		1	1		395 Bytes	0 Byte
	fe80::1459:d999:bf1c:26ee   	ff02::fb  	MDNS 	1		1	1		495 Bytes	0 Byte
	devel     	142.250.184.78    	G+ HTTP.Google ...	1	10	1	1	 	510 Bytes	1.02 KI
	devel     	_gateway     	DNS 	7	30	1	1	 	576 Bytes	875 Byte
	fe80::36db:fdff:fe80:d9a6    ...	ff02::1:2   	DHCPV6 	1		1	1		648 Bytes	0 Byte
	192.168.2.198     	239.255.255.250   	SSDP 	1	10	1	1		872 Bytes	0 Byte

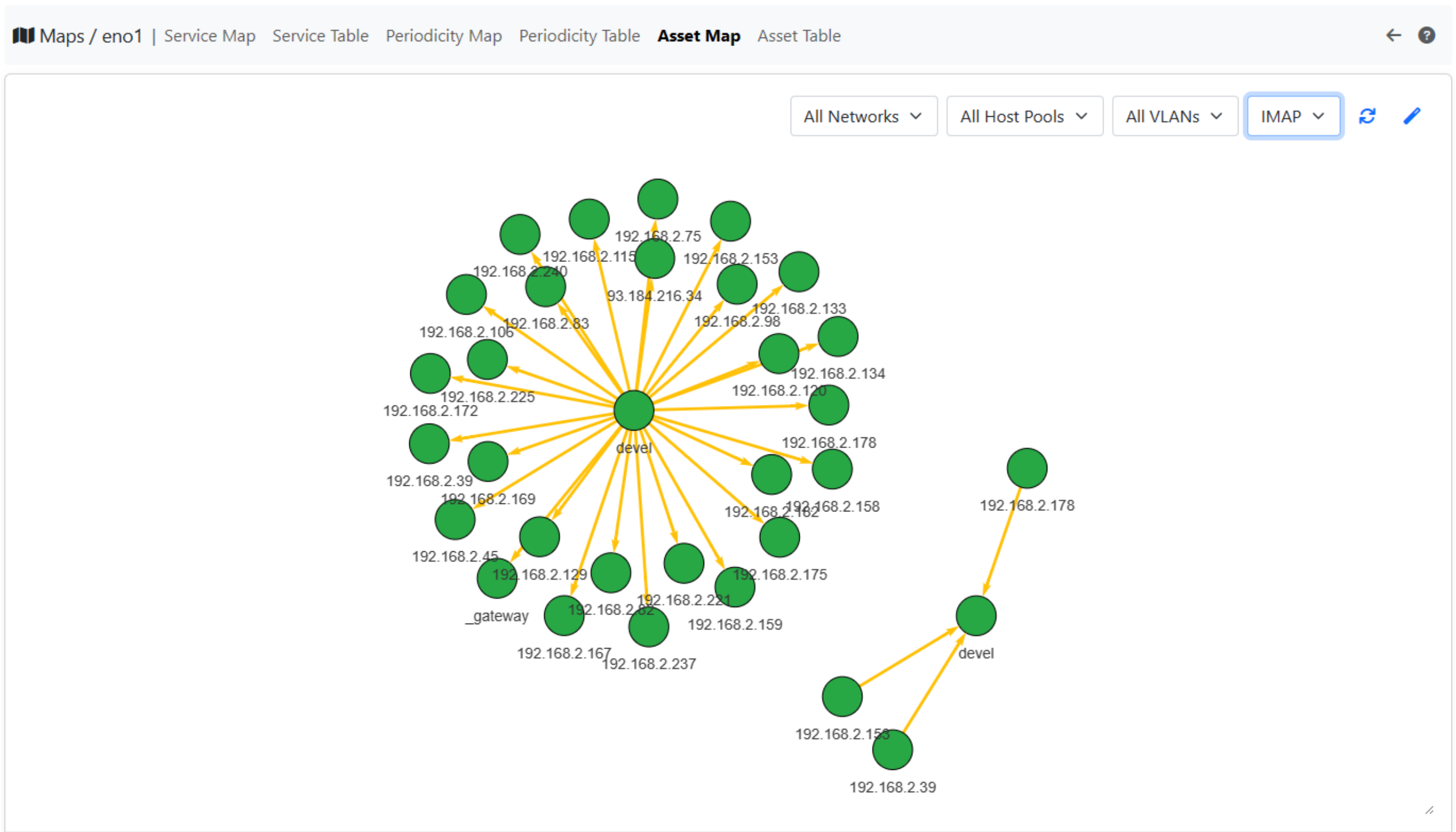
... & more Traffic Analysis



... & more Traffic Analysis



... & more Traffic Analysis



... & more Traffic Analysis

Hosts | Active Inactive Local Hosts 171

Table View Chart View

Show 20 Entries Device: All Manufacturer: All Network: All VLAN: All

Actions	Host	Name	MAC Address	Manufacturer	First Seen	Last Seen
	192.168.2.240@384 [Test vlan]		28:B1:33:00:59:4D	SHINEMAN(SHENZHEN) Tech. Cor., Ltd.	08/23/2023 16:00:44	08/23/2023 16:00:45
	192.168.2.240		28:B1:33:00:59:4D	SHINEMAN(SHENZHEN) Tech. Cor., Ltd.	15:28:44	15:28:45
	192.168.2.237@2223		00:04:96:E4:AA:CD	Extreme Networks, Inc.	08/23/2023 14:07:38	08/23/2023 14:07:39
	192.168.2.230		78:4F:43:59:14:68	Apple, Inc.	08/03/2023 14:51:15	08/03/2023 14:51:18
	192.168.2.225@384 [Test vlan]		00:E0:ED:1A:34:56	Silicom, Ltd.	08/23/2023 15:46:59	08/23/2023 15:47:07
	192.168.2.225		00:E0:ED:1A:34:56	Silicom, Ltd.	09/14/2023 11:20:21	09/14/2023 11:20:24
	192.168.2.222@3880	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	08/30/2023 13:47:26	08/30/2023 13:47:29
	192.168.2.222@3828	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	09/01/2023 10:15:50	09/01/2023 10:16:19
	192.168.2.222@3822	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	08/25/2023 13:00:51	08/25/2023 13:00:52
	192.168.2.222@3671	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	09/01/2023 10:00:14	09/01/2023 10:00:15
	192.168.2.222@3608	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	08/30/2023 09:00:34	08/30/2023 09:01:01
	192.168.2.222@3533	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	08/30/2023 08:19:22	08/30/2023 08:19:23
	192.168.2.222@3522	devel	00:25:90:D4:CC:F9	Super Micro Computer, Inc.	08/22/2023 16:45:01	08/22/2023 16:45:03

... & more Traffic Analysis



Vulnerability Scan (1/5)

- Analyze hosts in a network to discover vulnerabilities
- Discover open ports
- Manually or periodically scan single or multiple hosts

Vulnerability Scan (2/5)

Vulnerability Scan

Open Ports

Show 10 Entries

+ Search:

Actions	Host	Host Name	Scan Type	CVEs	TCP Ports	Last Scan Duration	Last Scan Date	Periodicity	Last Scan Status
	192.168.1.1	h388x.homenet.telecomitalia.it	CVE	3	6	02:24	12:19:29	Nightly	Success
	192.168.1.6	host-004.homenet.telecomitalia.it	CVE			00:02 sec	11:18:57	Nightly	Success
	192.168.1.10	host-002.homenet.telecomitalia.it	CVE	1,729	3	00:34 sec	11:26:05	Nightly	Success
	192.168.1.16		CVE			00:02 sec	12:16:55	Nightly	Success
	192.168.1.28	peppeasusi7.homenet.telecomitalia.it	CVE	5,518	3	00:08 sec	11:17:19	Nightly	Success
	192.168.1.30		CVE			00:02 sec	12:09:50	Nightly	Success
	192.168.1.88		CVE			00:02 sec	12:07:33	Nightly	Success
	192.168.1.110		CVE		5	02:00	11:16:27	Nightly	Success
	192.168.1.164		CVE			00:02 sec	12:08:17	Nightly	Success
	192.168.1.60		CVE			00:02 sec	11:13:39	Nightly	Success

Showing page 1 of 4: total 37 rows

< 1 2 3 4 >

Delete All

Schedule All Scans

Batch Edit

Vulnerability Scan (3/5)

- Download/Show Scan Report
- Schedule Periodic Scan
- Show CVEs (Vulnerabilities)
- Scan Hosts on specific ports

Vulnerability Scan (4/5)

Vulnerability Scan | 🏠 ⚠️ 📁 Open Ports Scan Details ←

Vulnerability Scan Report of 192.168.2.172 at 11:17:45

22/tcp open ssh Dropbear sshd 2013.60 (protocol 2.0)

vulscan: cve.csv:

[CVE-2012-0920] Use-after-free vulnerability in Dropbear SSH Server 0.52 through 2012.54, when command restriction and public key authentication are enabled, allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certain proof of concept.
[CVE-2009-3340] Unspecified vulnerability in FreeSSH 1.2.4 allows remote attackers to cause a denial of service via unknown vectors, as demonstrated by a certain proof of concept.
[CVE-2008-3234] sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows remote authenticated users to obtain access to arbitrary SELinux processes.
[CVE-2006-5794] Unspecified vulnerability in the sshd Privilege Separation Monitor in OpenSSH before 4.5 causes weaker verification that authentication has been successful.
[CVE-2006-1283] opiepasswd in One-Time Passwords in Everything (OPIE) in FreeBSD 4.10-RELEASE-p22 through 6.1-STABLE before 20060322 uses the getlogin function to verify the user name.
[CVE-2002-0460] Bitwise WinSSHD before 2002-03-16 allows remote attackers to cause a denial of service (resource exhaustion) via a large number of incomplete connections.

80/tcp open http ATEN/Supermicro IPMI web interface

vulscan: cve.csv:

[CVE-2013-4785] The web interface for Dell iDRAC 6 firmware 1.7, and possibly other versions, allows remote attackers to modify the CLP interface for arbitrary commands.
[CVE-2013-4731] ajax.cgi in the web interface on the Choice Wireless Green Packet WIXFMR-111 4G WiMax modem allows remote attackers to execute arbitrary commands.
[CVE-2013-4620] Cross-site scripting (XSS) vulnerability in interface/main/notes/officecommentsfull.php in OpenEMR 4.1.1 allows remote attackers to inject arbitrary JavaScript.
[CVE-2013-4038] The Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) on IBM BladeCenter, Flex System, System x3500 M3, and System x3600 M3 allows remote attackers to execute arbitrary commands.
[CVE-2013-4037] The RAKP protocol support in the Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) and Integrated Management Module II (IMM2) on IBM BladeCenter, Flex System, System x3500 M3, and System x3600 M3 allows remote attackers to execute arbitrary commands.
[CVE-2013-4031] The Intelligent Platform Management Interface (IPMI) implementation in Integrated Management Module (IMM) and Integrated Management Module II (IMM2) on IBM BladeCenter, Flex System, System x3500 M3, and System x3600 M3 allows remote attackers to execute arbitrary commands.
[CVE-2013-3633] The web interface on Siemens Scalance X200 IRT switches with firmware before X-200IRT 5.1.0 relies on client-side privilege checks, which allows remote attackers to execute arbitrary commands.
[CVE-2013-3581] ajax.cgi in the web interface on the Choice Wireless Green Packet WIXFMR-111 4G WiMax modem allows remote attackers to obtain sensitive information.
[CVE-2013-3500] The Foundation webapp admin interface in GroundWork Monitor Enterprise 6.7.0 uses the nagios account as the owner of writable files under /usr/local, which allows remote attackers to execute arbitrary commands.
[CVE-2013-3457] Absolute path traversal vulnerability in the web interface in Cisco Finesse allows remote attackers to read directory contents via a direct request.
[CVE-2013-3440] Multiple cross-site scripting (XSS) vulnerabilities in the administrative web interface in Cisco Unified Operations Manager allow remote attackers to execute arbitrary JavaScript.
[CVE-2013-3428] The web interface in Cisco Secure Access Control System (ACS) does not properly suppress error-condition details, which allows remote attackers to execute arbitrary JavaScript.
[CVE-2013-3423] Cross-site scripting (XSS) vulnerability in the web interface in Cisco Secure Access Control System (ACS) allows remote attackers to inject arbitrary JavaScript.
[CVE-2013-3380] The administrative web interface in the Access Control Server in Cisco Secure Access Control System (ACS) does not properly restrict the report of error messages.
[CVE-2013-3080] VMware vCenter Server Appliance (vCSA) 5.1 before Update 1 allows remote authenticated users to create or overwrite arbitrary files, and consequently cause a denial of service.

Vulnerability Scan (5/5)

Vulnerability Scan | Open Ports

Show 10 Entries Search:

Actions	Port	Service Name	CVEs	Count	Hosts
	22	ssh	52,767	23	192.168.2.225, 192.168.2.221, 192.168.2.222, 192.168.2.106, 192.168.2.153...
	80	http	53,402	16	192.168.2.221, 192.168.2.106, 192.168.2.167, 192.168.2.120, 192.168.2.133...
	443	https	42,569	12	192.168.2.221, 192.168.2.167, 192.168.2.120, 192.168.2.133, 192.168.2.60...
	3000	remoteware-cl	485	6	192.168.2.222, 192.168.1.60, 192.168.2.240, 192.168.2.178, 192.168.2.134...
	5900	rfb	41,952	5	192.168.2.120, 192.168.2.133, 192.168.2.158, 192.168.2.172, 192.168.2.83
	9090	websm	59	4	192.168.2.221, 192.168.2.240, 192.168.2.134, 192.168.2.75
	9000	cslistener	474	4	192.168.2.39, 192.168.1.110, 192.168.2.178, 192.168.2.134
	53	domain	204	4	192.168.2.60, h388x.homenet.telecomitalia.it, 192.168.2.1, 192.168.2.59
	23	telnet	10,632	3	192.168.2.106, 192.168.2.169, 192.168.2.237
	135	epmap	5,518	3	peppeasusi7.homenet.telecomitalia.it, 192.168.1.30, 192.168.1.16

Showing page 1 of 4: total 40 rows

< 1 2 3 4 >

Local Traffic Rules (1/3)

Monitoring SNMP devices / Hosts / Interfaces to unveil changes in traffic:

- Check periodically (every 5 mins, 1 hour, or 1 day) timeseries.
- Multiple metrics to check available (Traffic, Apps, Score, ...)
- When a configured Threshold is exceeded



Trigger an alert

(Available only from Enterprise L license)

Local Traffic Rules (2/3)

Local Traffic Rules

Show 10 entries

What to Monitor

Target	Type	Metric	Check Frequency	Last Measurement	Threshold	Actions
eno1	Interface	Score	Hourly	506290	5000	
eno1	Interface	Traffic	5 Minutes	2.82 MB	< 3 GB	
192.168.2.1	Host	DNS	5 Minutes	7.60 Mbps	< 125.00 Kbps	
*	Host	Traffic	5 Minutes		< 1 GB	

Threshold

Frequency

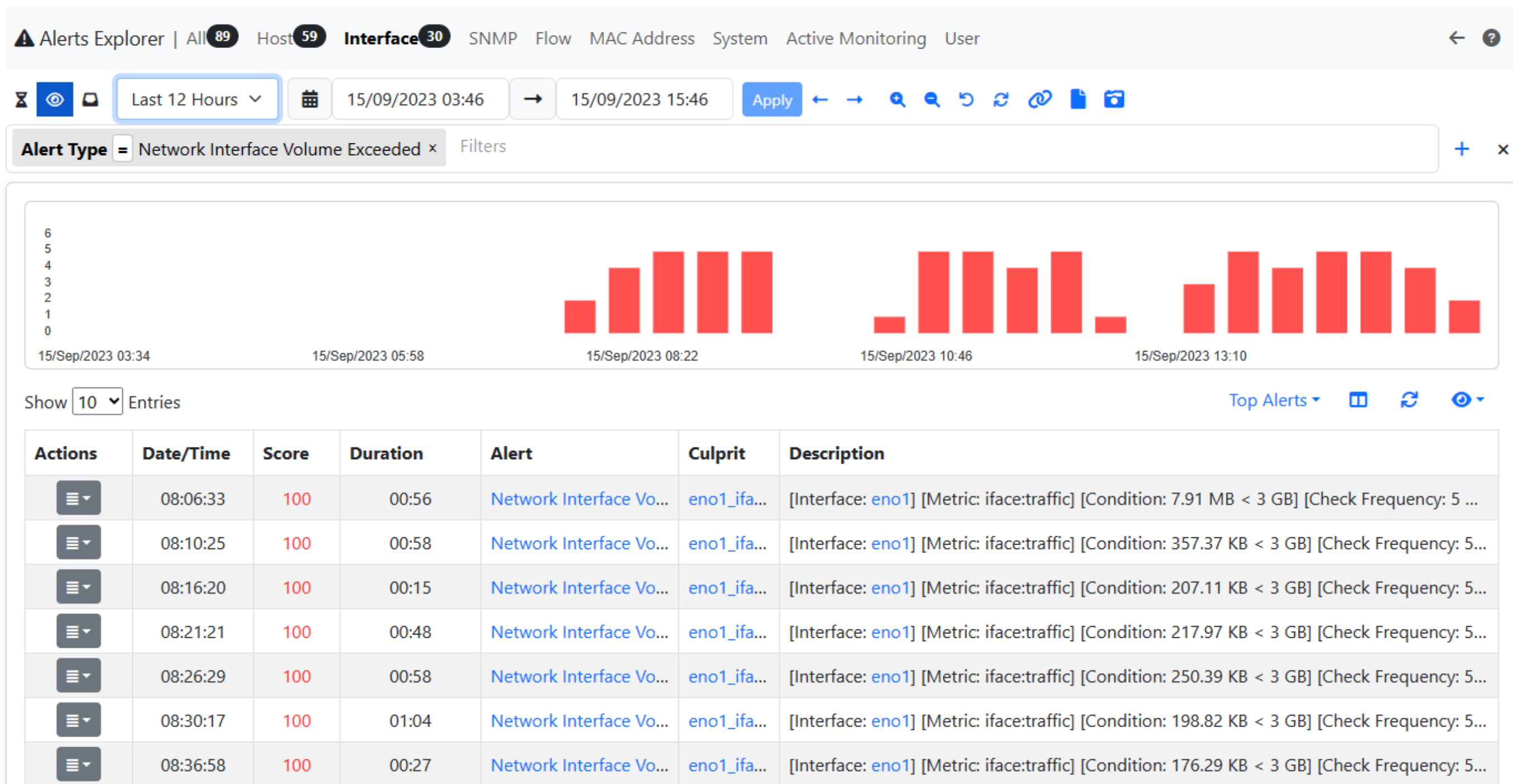
Showing 1 to 4 of 4 entries

« < 1 > »

NOTES

- Trigger an alert when a local host exceeds the specified traffic amount
- To add a new rule, click the '+' symbol on the right side above the table (next to the search)
- To remove a rule, click on the 'Actions' column button and then click onto 'Delete' on the row you want to remove

Local Traffic Rules (3/3)



Integrations

Before:

- Discord
- Elasticsearch
- E-Mail
- Fail2Ban
- Slack
- Syslog
- Teams
- Telegram
- Webhook

Now:

- Discord
- Elasticsearch
- E-Mail
- Fail2Ban
- Mattermost
- PagerDuty
- Slack
- Syslog
- Teams
- Telegram
- TheHive
- Webhook

Integrations

- PagerDuty is one of the most commonly used software solutions for managing notifications
- TheHive a wide known platform for managing cybersecurity alerts
- Mattermost one of the most used business chat platforms

TheHive

The screenshot displays the 'Platform Management' section of TheHive, specifically the 'Platform status' page. The 'Status' tab is selected, showing the 'Database Schema status' and 'Database integrity check' sections.

Database Schema status

Status	Schema name	Schema version
OK	thehive-enterprise	67
OK	thehive	98
OK	thehive-cortex	2

Database integrity check

Control name	#Entities	
Action	0	See details
Alert	1052	See details
AlertStatus	7	See details
AnalyzerTemplate	214	See details

A red rounded rectangle highlights the 'Alert' row in the 'Database integrity check' table. A blue arrow points from the text below to this row. The version '5.1.9-1' is visible in the bottom left corner of the interface.

Sending notifications to TheHive the Alert Entities count will increase

PagerDuty

PagerDuty

Incidents

Services

People

Automation

Analytics

Integrations

Status

 Search

Incidents on All Teams

Your open incidents

198 triggered

12 acknowledged

All open incidents

198 triggered

12 acknowledged

 Acknowledge

 Reassign

 Resolve

 Snooze ▾

Go to incident #...

 All Teams

Open

Triggered





Acknowledged

Resolved

Any Status

Assigned to me

All

<input type="checkbox"/>	Status	Priority ▾	Urgency ▴	Title		Created ▴	Service	Assigned To
<input type="checkbox"/>	Triggered	--	High	[System]: Process  SHOW DETAILS (1 triggered alert)	#210	on Aug 16, 2023 at 5:33 PM	ntopng_service	Nicolo' Maio
<input type="checkbox"/>	Triggered	--	High	[Flow]: Known Proto on Non Std Port  SHOW DETAILS (1 triggered alert)	#209	on Aug 16, 2023 at 5:29 PM	ntopng_service	Nicolo' Maio
<input type="checkbox"/>	Triggered	--	High	[Flow]: Known Proto on Non Std Port  SHOW DETAILS (1 triggered alert)	#208	on Aug 16, 2023 at 5:29 PM	ntopng_service	Nicolo' Maio
<input type="checkbox"/>	Triggered	--	High	[Flow]: Known Proto on Non Std Port  SHOW DETAILS (1 triggered alert)	#207	on Aug 16, 2023 at 5:29 PM	ntopng_service	Nicolo' Maio

nEdge

ntopng inline, designed to solve a few problems:

- Bind devices to users
- Specify per-user application protocol policies
- Protect the network from malware and connections
- Make sure that the available Internet bandwidth is shared evenly

nEdge Updates

- Added support for multi-LAN
- Added support for VLANs
- Added handling of DHCPd Service
- Improved RADIUS AUTH
- Added RADIUS ACCT



Sept, 21-22 · Pisa