

ntop MiniConference 2021: ntopng News and Updates

Matteo Biscosi
biscosi@ntop.org



Agenda

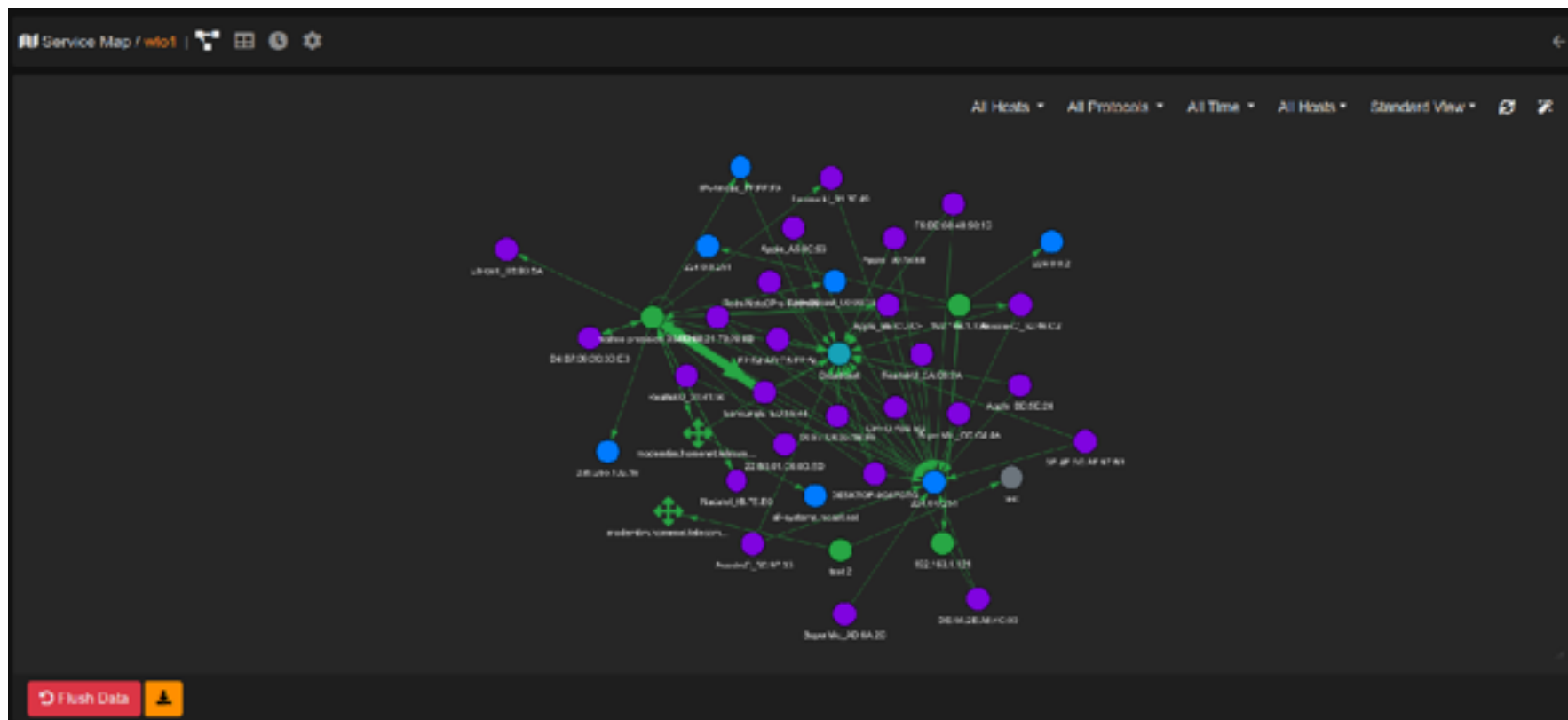
- Today's talk, everything about 2021
 - ntopng 5.0: What's new
 - ntopng 5.1: Latest news and Updates
 - nEdge: News
 - Demo

ntopng 5.0: What's new

Improvements to Network Visibility and Alerting System

Service & Periodicity Maps

- Check Services
 - Learning period
 - Service Status
- Check Periodic Flows

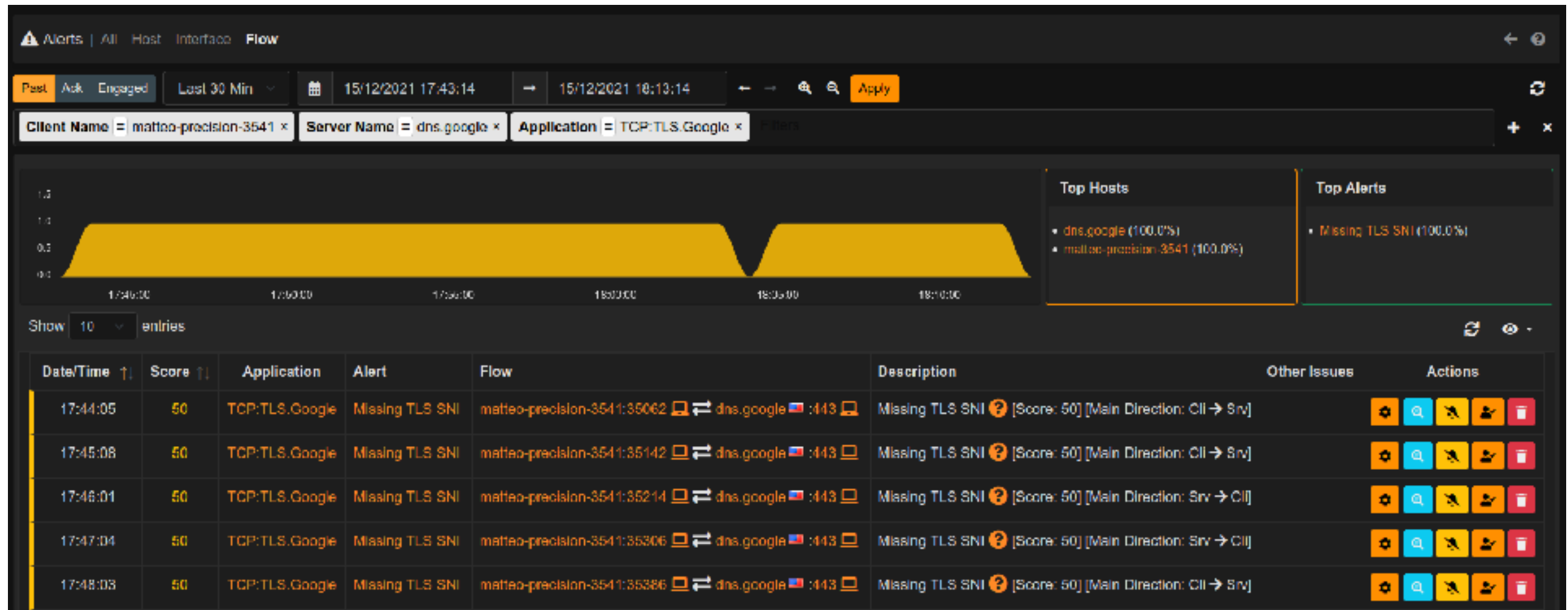


Alerts (Checks) [1/2]

Revamp of Alert (Checks) Page

- New Alert Page
 - Advanced filtering system
 - Past/Acknowledged/Engaged alerts
- Exclusion List
- Attacker and Victim

Alerts (Checks) [2/2]



Score, key to the Severity

Indicator varying between 0 and 250 representing the danger (from 0 to 250)

- Host
- Flows

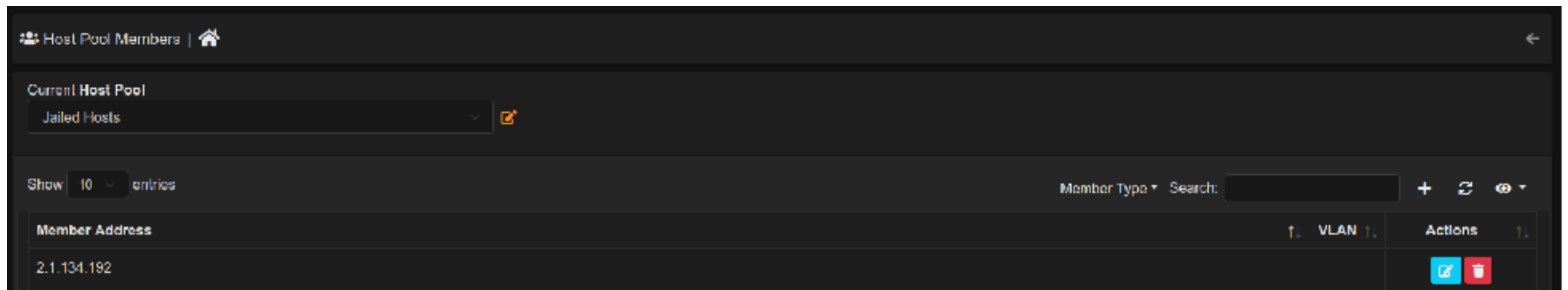
This screenshot shows the ntopng interface for a specific host. The host is identified as 'matteo-precision-3541'. Key details include:

- MAC Address:** E4:5E:37:AF:C9:E0 (Unknown Device Type)
- IP Address:** 192.168.1.77 (Host Pool: Test pool)
- OS:** Linux [Ubuntu]
- Name:** matteo-precision-3541
- Score:** 40 (Visualized as a bar chart with 'Network' in yellow and 'Circumlocution' in green)

Date/Time	Score	Application	Alert	Flow	Actions
03/12/2021 14:19:30	250	TCP:HTTP:UbuntuONE	Binary Application Trans...	matteo-precision-3541.ho...:35526 → it.archive.ubuntu.com :80	    
Description: Detected binary application transfer [it.archive.ubuntu.com/ubuntu/pool/main/v/vim/vim-runtime_8.2.071...] [Score: 250] [Method: GET] [Return Code: 20...]					
Other Issues					

Jailed Host Pool

- Dangerous Host
 - Alert if an Host exceeds a Threshold
 - Automatically ban an Host for 30 minutes with nProbe IPS mode



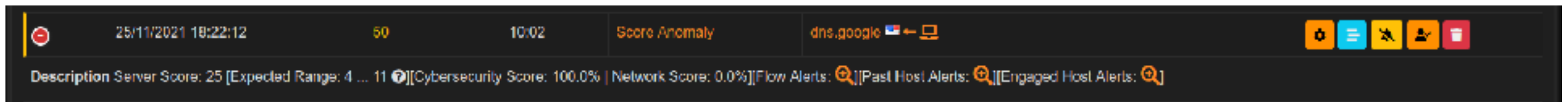
The screenshot shows the 'Host Pool Members' page in ntopng. The 'Current Host Pool' is set to 'Jailed Hosts'. The table displays one member with the address 2.1.134.192. The interface includes a search bar, a 'Member Type' dropdown, and a table with columns for 'Member Address', 'VLAN', and 'Actions'.

Member Address	VLAN	Actions
2.1.134.192		 

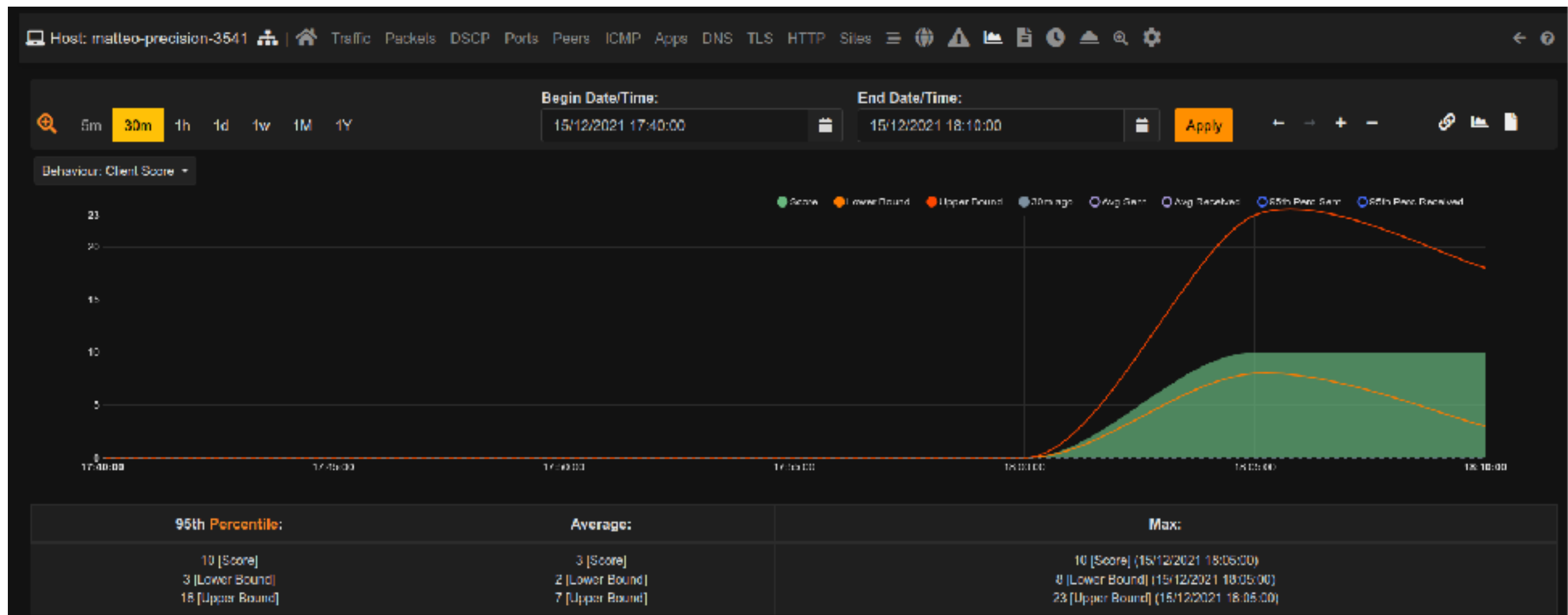
Checks and Anomaly Checks [1/2]

Introduced new checks with ntopng 5.0 and 5.1 versions

- Anomaly Checks



Checks and Anomaly Checks [2/2]

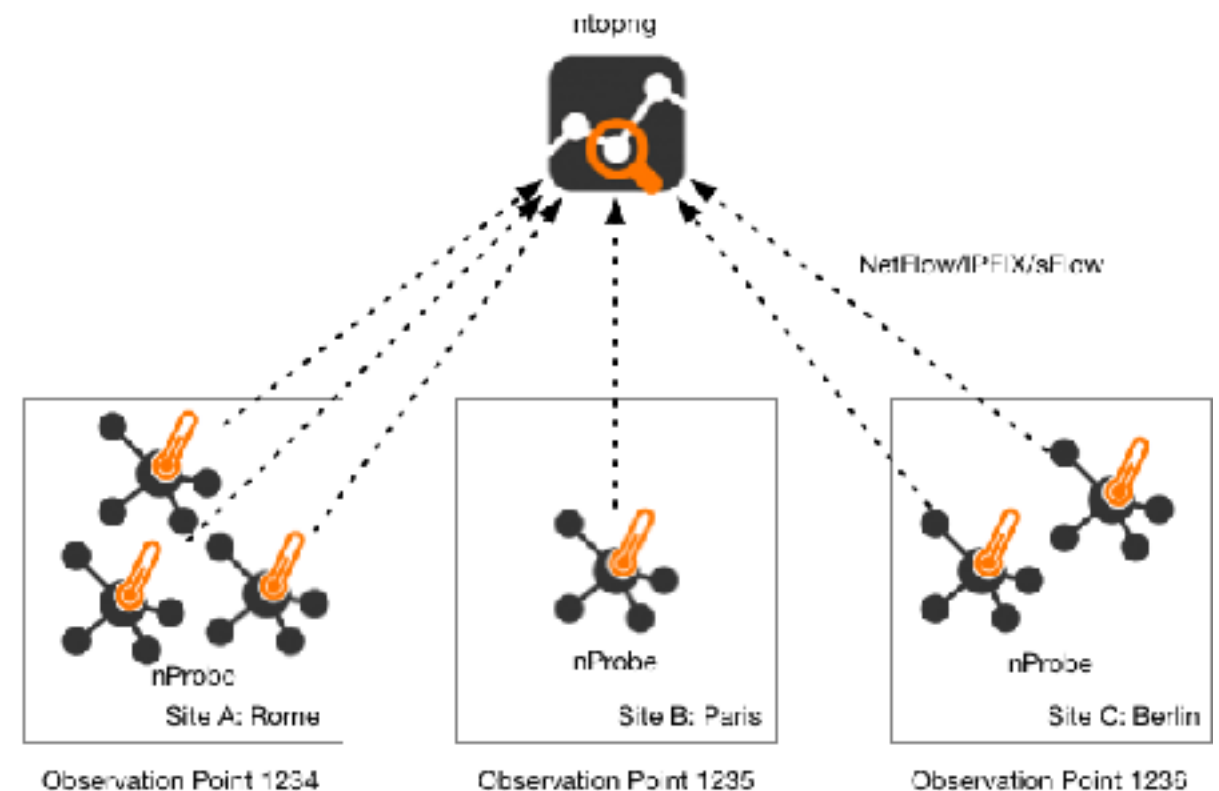


Improving Flow Visibility and Flow Analysis

Observation Points

A location in the Network where packets can be observed.

Multiple Observation points can be used per Interface.

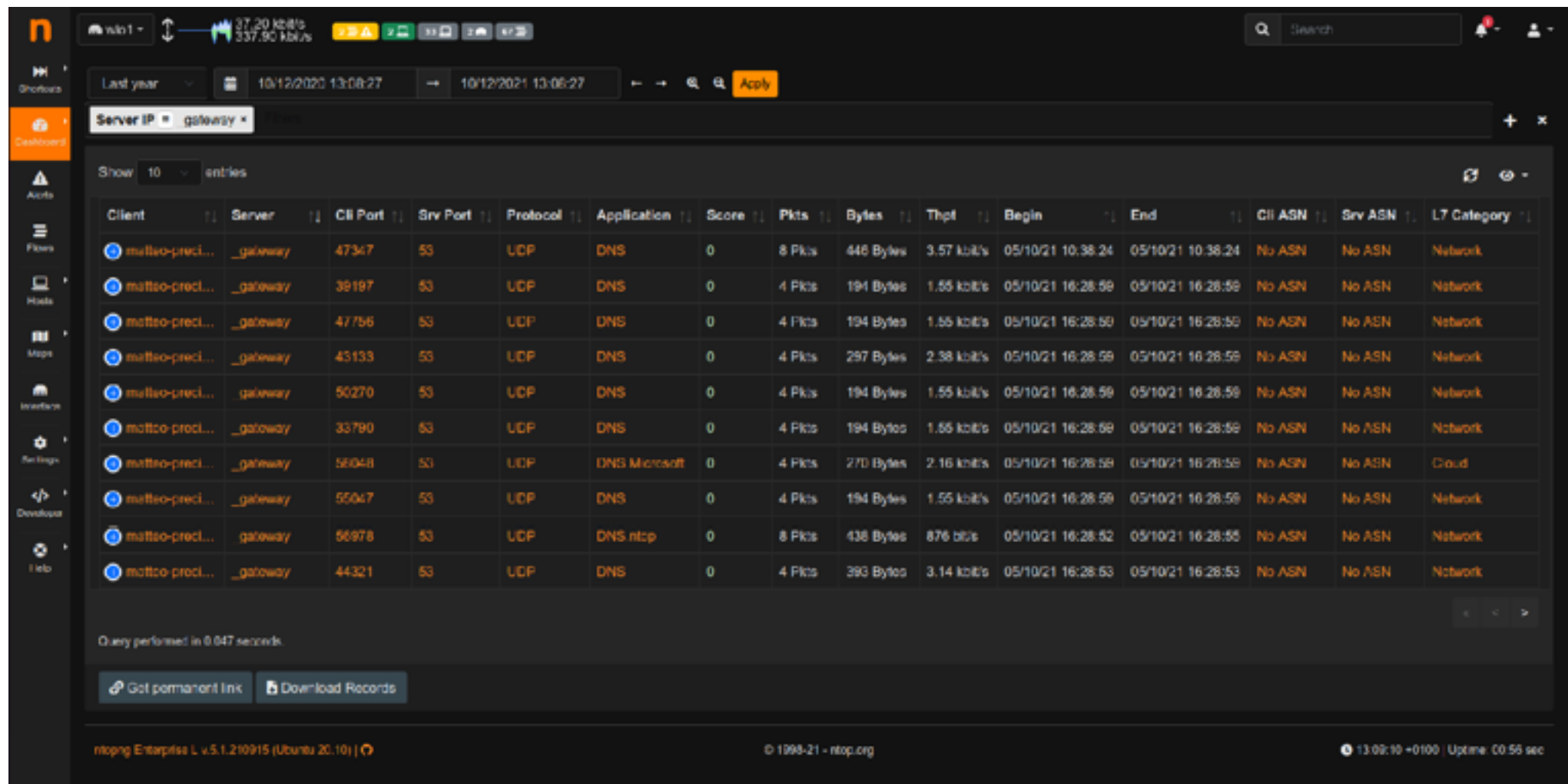


The screenshot shows the ntopng web interface. At the top, there's a status bar with network statistics. Below that, the 'Recently Active Flows' section is visible. It contains a table with columns: Application, Protocol, Client, Server, First Seen, Last Seen, Score, Breakdown, Actual Thpt, Total Bytes, and Info. Two flows are listed: ICMPV6 and DNS.Github.

Application	Protocol	Client	Server	First Seen	Last Seen	Score	Breakdown	Actual Thpt	Total Bytes	Info
ICMPV6	IPv6-ICMP	matteo-precision-3541	fe80::22b0:1ff:fe06:de4	10/12/2021 12:20:59	10/12/2021 12:20:59	100%	Client Server	0 bps	136 Bytes	Reserved
DNS.Github	UDP	matteo-precision-3541	fe80::22b0:1ff:fe06:de4	10/12/2021 12:20:54	10/12/2021 12:20:54	100%	Client Server	0 bps	174 Bytes	github.com

Historical Flow Explorer

A way to visualize, filter and sort out the flows flowing through the network (feature supported by nIndex).



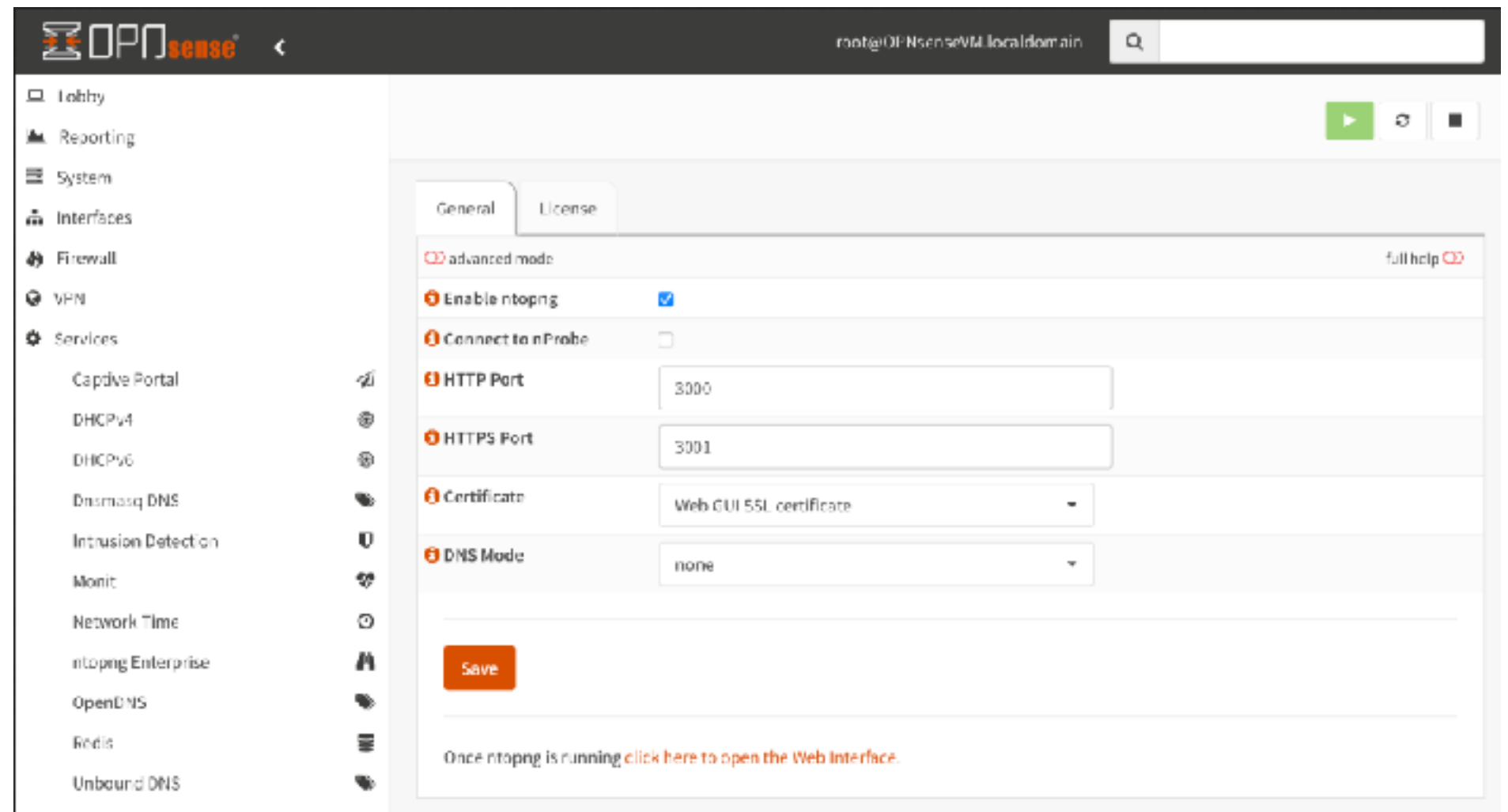
The screenshot displays the ntop Historical Flow Explorer interface. At the top, there's a navigation bar with the ntop logo, a search bar, and a date range selector set to 'Last year' with specific dates '10/12/2020 13:08:27' and '10/12/2021 13:08:27'. Below this, a filter bar shows 'Server IP' set to 'gateway'. The main area contains a table of network flows with columns for Client, Server, Cll Port, Srv Port, Protocol, Application, Score, Pkts, Bytes, Thpt, Begin, End, Cll ASN, Srv ASN, and L7 Category. The table lists several DNS flows from 'matteo-precl...' to 'gateway' on port 53, with various applications like 'DNS', 'DNS Microsoft', and 'DNS ntp'. At the bottom, there are buttons for 'Get permanent link' and 'Download Records', and a footer with version information and uptime.

Client	Server	Cll Port	Srv Port	Protocol	Application	Score	Pkts	Bytes	Thpt	Begin	End	Cll ASN	Srv ASN	L7 Category
matteo-precl...	_gateway	47367	53	UDP	DNS	0	8 Pkts	446 Bytes	3.57 kbit/s	05/10/21 10:38:24	05/10/21 10:38:24	No ASN	No ASN	Network
matteo-precl...	_gateway	39197	53	UDP	DNS	0	4 Pkts	194 Bytes	1.55 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	47756	53	UDP	DNS	0	4 Pkts	194 Bytes	1.55 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	43133	53	UDP	DNS	0	4 Pkts	297 Bytes	2.38 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	50270	53	UDP	DNS	0	4 Pkts	194 Bytes	1.55 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	33790	53	UDP	DNS	0	4 Pkts	194 Bytes	1.55 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	58048	53	UDP	DNS Microsoft	0	4 Pkts	270 Bytes	2.16 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Cloud
matteo-precl...	_gateway	55067	53	UDP	DNS	0	4 Pkts	194 Bytes	1.55 kbit/s	05/10/21 16:28:59	05/10/21 16:28:59	No ASN	No ASN	Network
matteo-precl...	_gateway	56978	53	UDP	DNS ntp	0	8 Pkts	438 Bytes	876 bit/s	05/10/21 16:28:52	05/10/21 16:28:52	No ASN	No ASN	Network
matteo-precl...	_gateway	44321	53	UDP	DNS	0	4 Pkts	393 Bytes	3.14 kbit/s	05/10/21 16:28:53	05/10/21 16:28:53	No ASN	No ASN	Network

new Distro

Added ntopng support to 3 new distro

- pfSense
- OPNsense
- FreeBSD

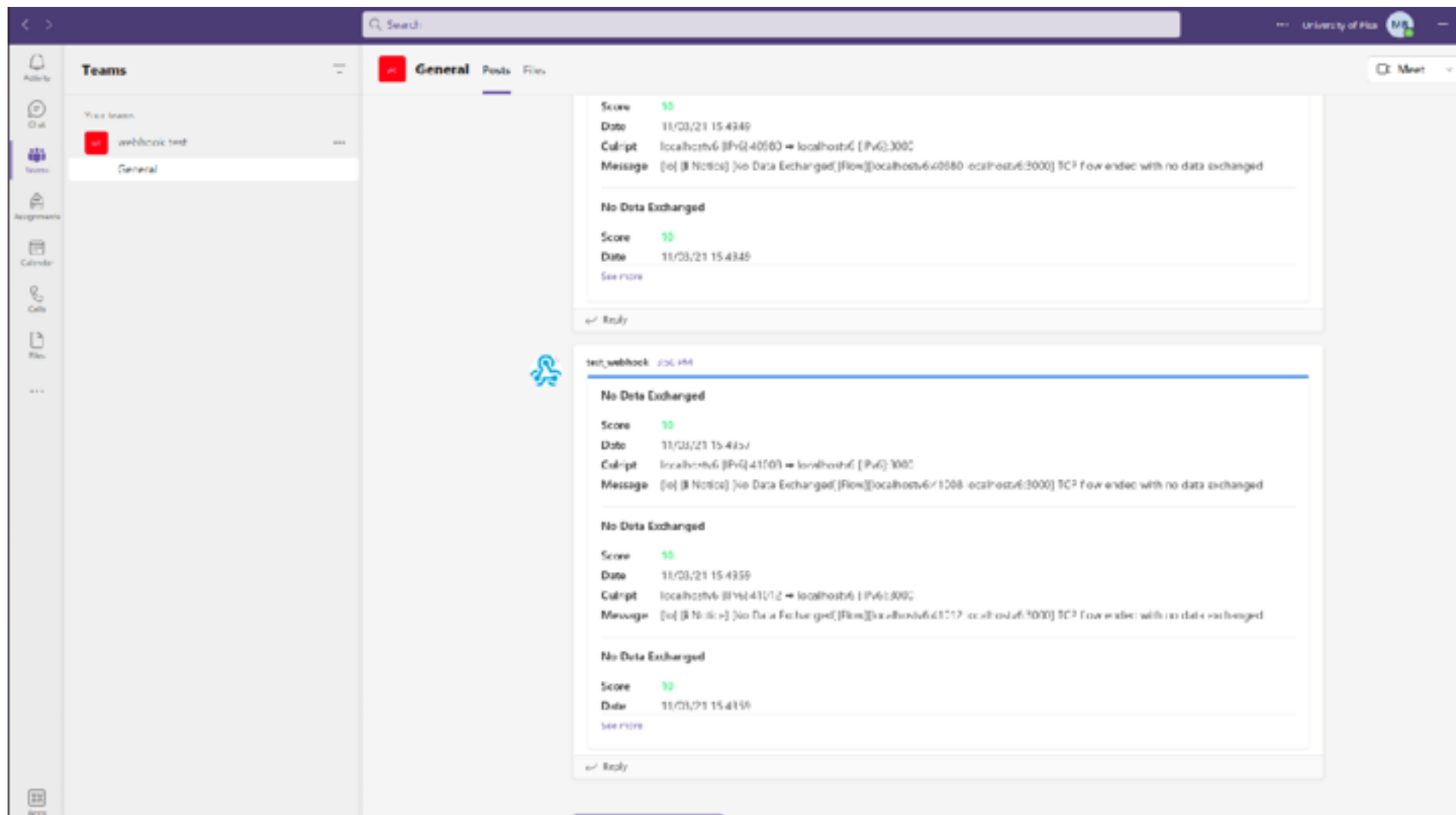


Demo

ntopng 5.1: Latest news and Updates

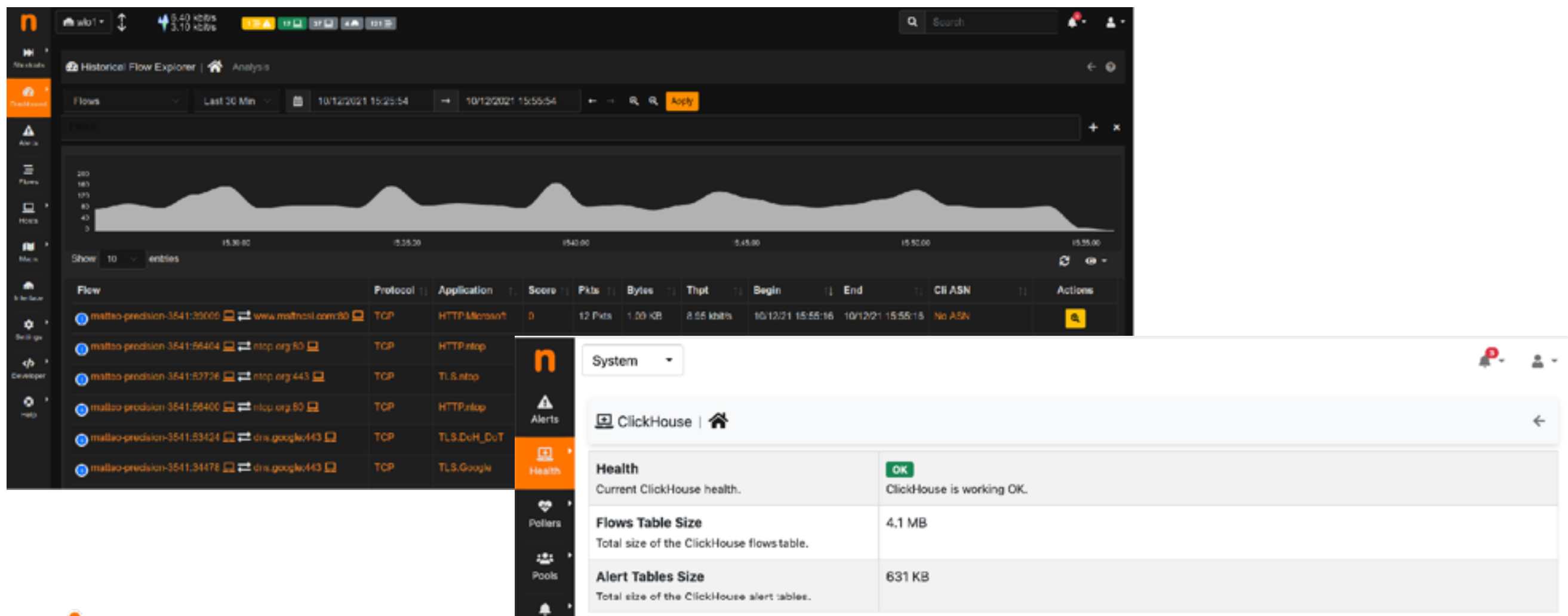
MS Teams Endpoint

Microsoft Teams Endpoint support added.



ClickHouse support

Added ClickHouse DB support for both Alerts and Flows (Migration from nIndex to CH supported, check <https://www.ntop.org/guides/ntopng/clickhouse.html>).

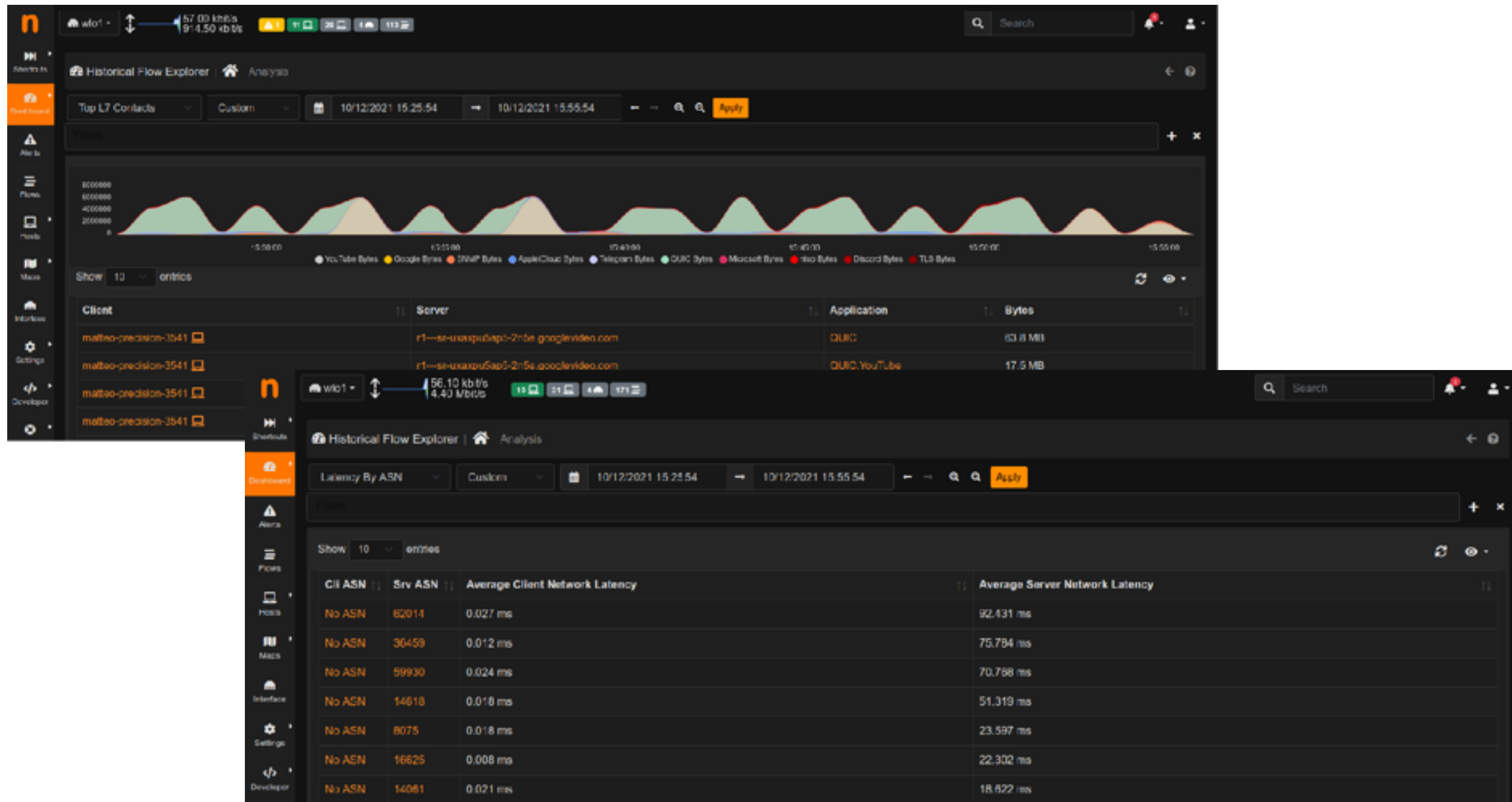


Historical Flow Explorer Revamp [1/2]

With ClickHouse introduction

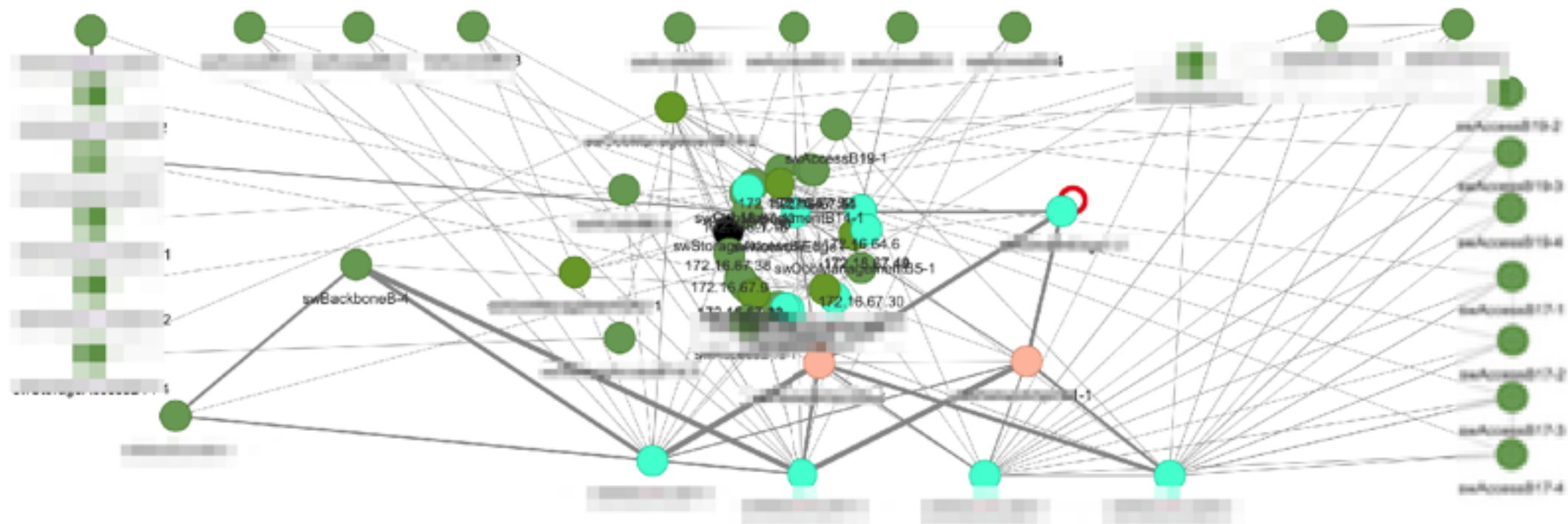
- New and more functional Historical Flow Explorer page GUI
- Support to other Queries added
 - Top L7 Contacts
 - Top Clients
 - Latency by ASN
 - ...

Historical Flow Explorer Revamp [2/2]



SNMP Improvements

- Support for the Cisco Discovery Protocol (CDP) to create network topologies
- Faster device polling



SNMP Similarity

- Spot timeseries similarity
 - e.g., “Is load balancing working as it should?”

SNMP Devices | Interfaces   

Network Interfaces Traffic Similarity

10 -

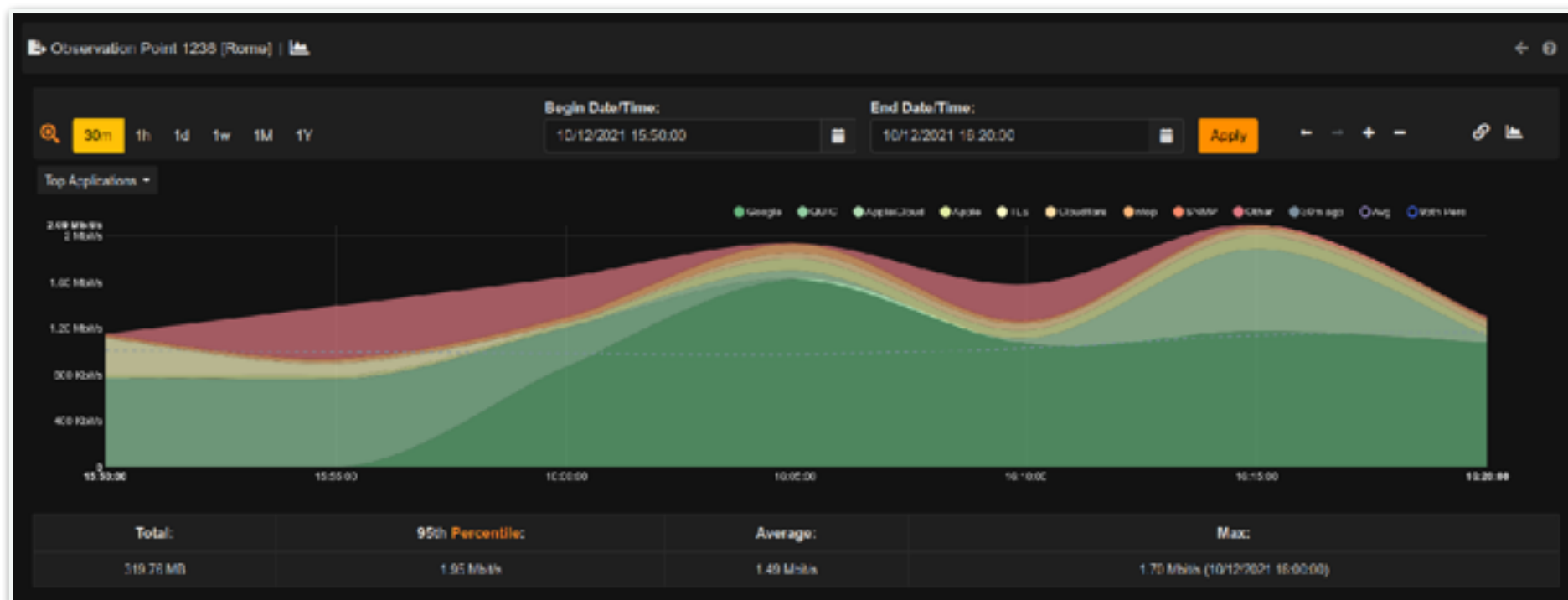
SNMP Device A	Interface Index A	Average Traffic A	SNMP Device B	Interface Index B	Average Traffic B	Similarity Score
318-4	2100867 (GigabitEthernet 1/30)	31.27 kbit/s	18-4	2100739 (GigabitEthernet 1/30)	31.27 kbit/s	100.0
319-4	2099459 (GigabitEthernet 1/19)	6.38 kbit/s	19-4	2099203 (GigabitEthernet 1/19)	6.38 kbit/s	100.0
317-2	2098819 (GigabitEthernet 1/14)	84.04 kbit/s	17-2	2098563 (GigabitEthernet 1/14)	84.04 kbit/s	99.0
neB-4	2099331 (GigabitEthernet 1/18)	39.64 kbit/s	neB-4	2099203 (GigabitEthernet 1/18)	39.64 kbit/s	99.0
AccessB14-4	2101251 (GigabitEthernet 1/33)	797.78 bit/s	AccessB14-4	2101123 (GigabitEthernet 1/33)	797.67 bit/s	98.3
AccessB4-1	2099203 (GigabitEthernet 1/17)	791.44 bit/s	AccessB4-1	2098947 (GigabitEthernet 1/17)	791.56 bit/s	98.3
AccessB14-4	2100867	797.69 bit/s	AccessB14-4	2101507	797.89 bit/s	98.0
AccessB14-4	2100611	75.28 kbit/s	AccessB14-4	2100739	75.28 kbit/s	97.8
AccessB4-1	2099331	792.22 bit/s	AccessB4-1	2098819	792.11 bit/s	97.8
neB-4	1258297856	21.15 kbit/s	neB-4	1258298369	21.15 kbit/s	97.8

Showing 1 to 10 of 1489 rows

« < 1 2 3 4 5 > »

Observation Points Timeseries

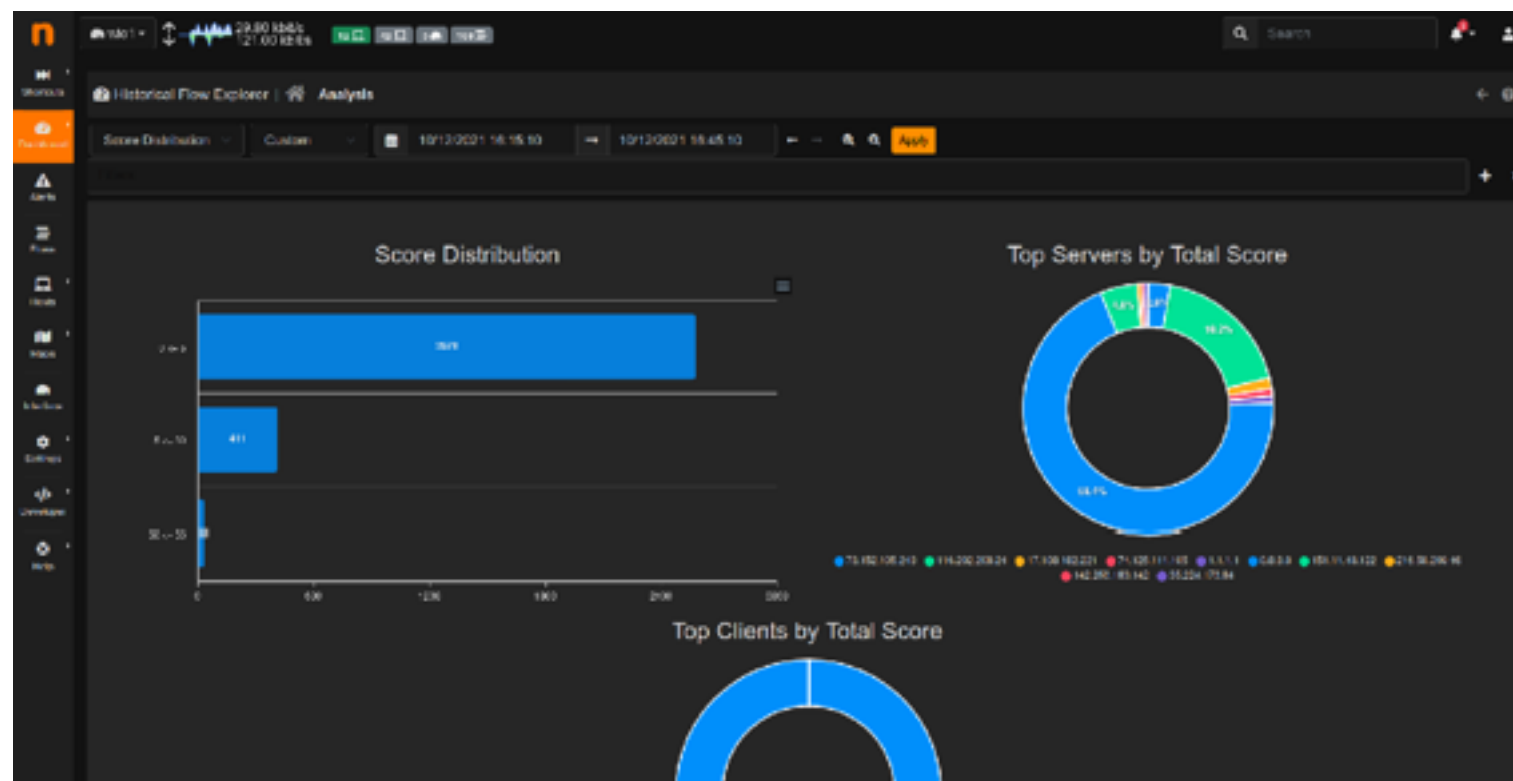
- Application Timeseries
- Score Timeseries
- Top Application Timeseries



Demo

ntopng Future Thoughts and Future Directions

- Removal of nIndex DB support
- Revamp of Traffic Report
- Historical Flow Explorer: Own your Graphs
- Observation Points Enhancement and per-Points stats



nEdge News

- Added ntopng security indicators
 - Score
 - Periodicity and service maps
- Introduced SNMP support
- Added metrics to count userspace vs. total traffic
 - “How effective is nEdge in offloading the traffic?”
- List currently active DHCP leases in router mode
- Daily, weekly and monthly quotas