ntop MiniConference 2021: ntopng News and Updates

Matteo Biscosi
biscosi@ntop.org

Agenda

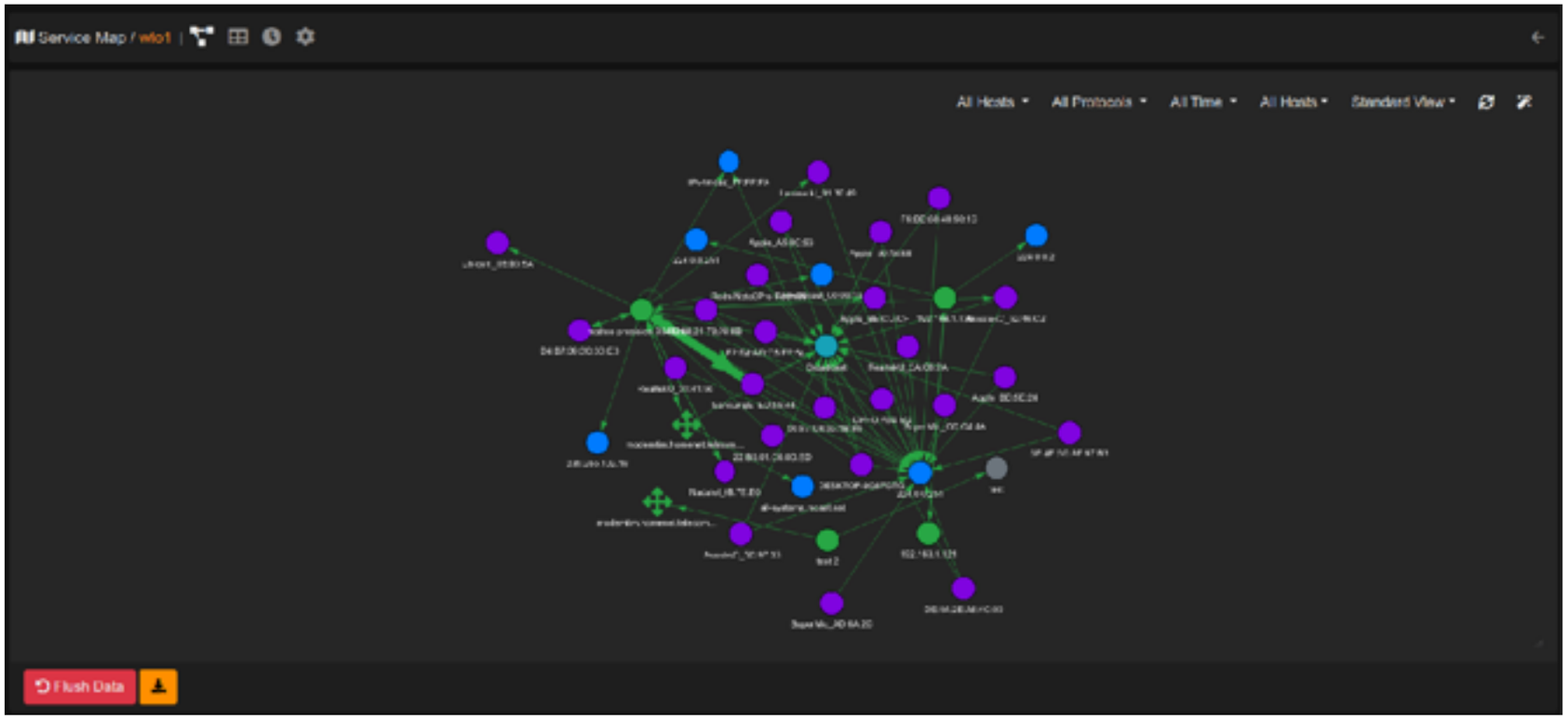
- Today's talk, everything about 2021
  - ntopng 5.0: What's new
  - ntopng 5.1: Latest news and Updates
  - nEdge: News
  - Demo

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

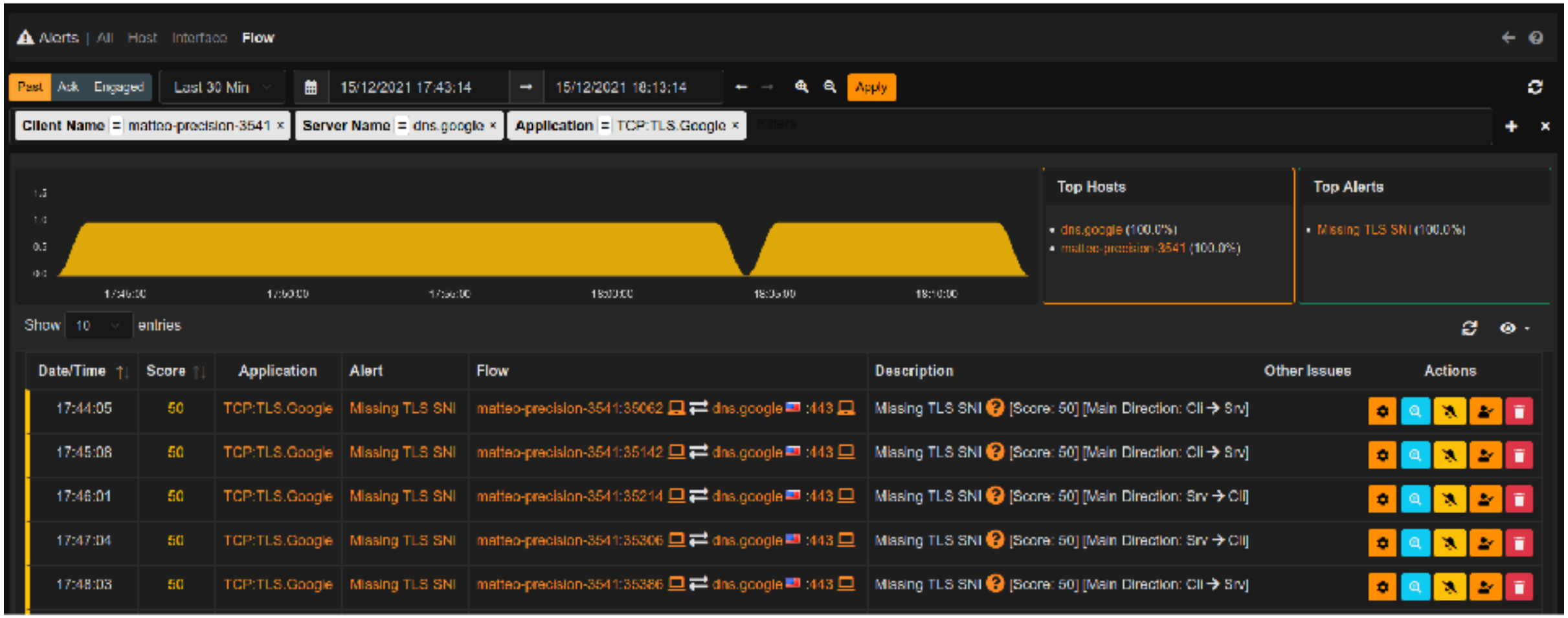


Alerts (Checks) [1/2]

Revamp of Alert (Checks) Page

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

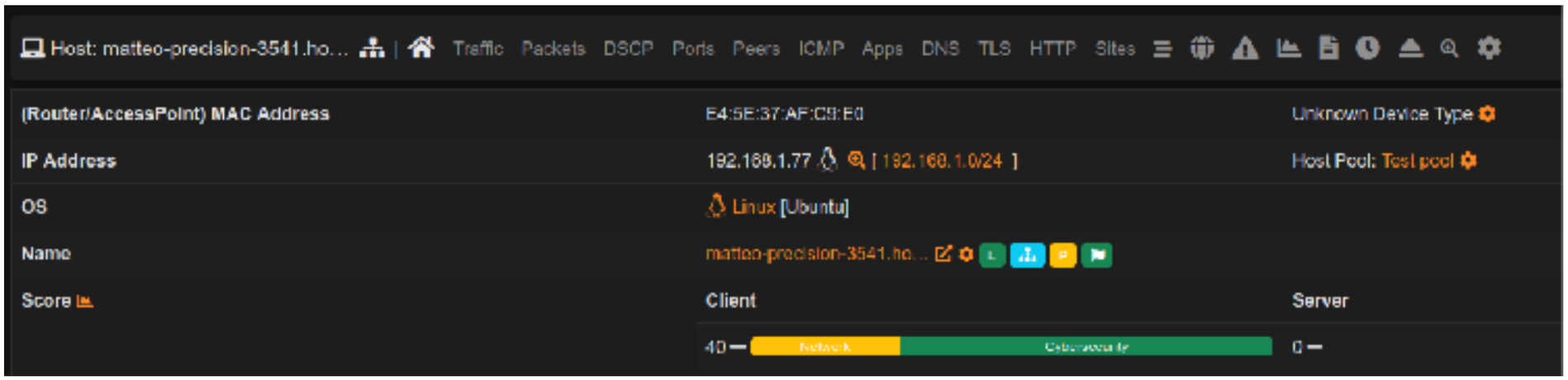
Alerts (Checks) [2/2]

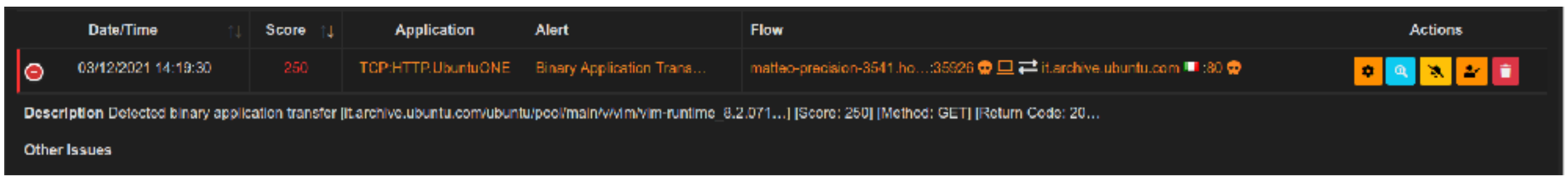


Score, key to the Severity

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

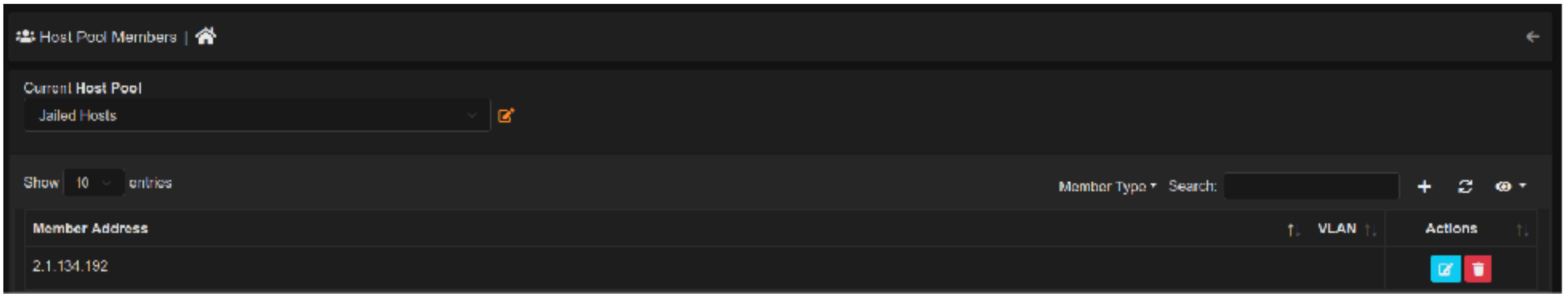
- Host
- Flows





Jailed Host Pool

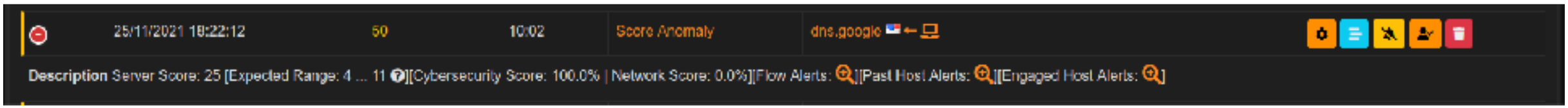
- Dangerous Host
  - Alert if an Host exceeds a Threshold
  - Automatically ban an Host for 30 minutes with nProbe IPS mode



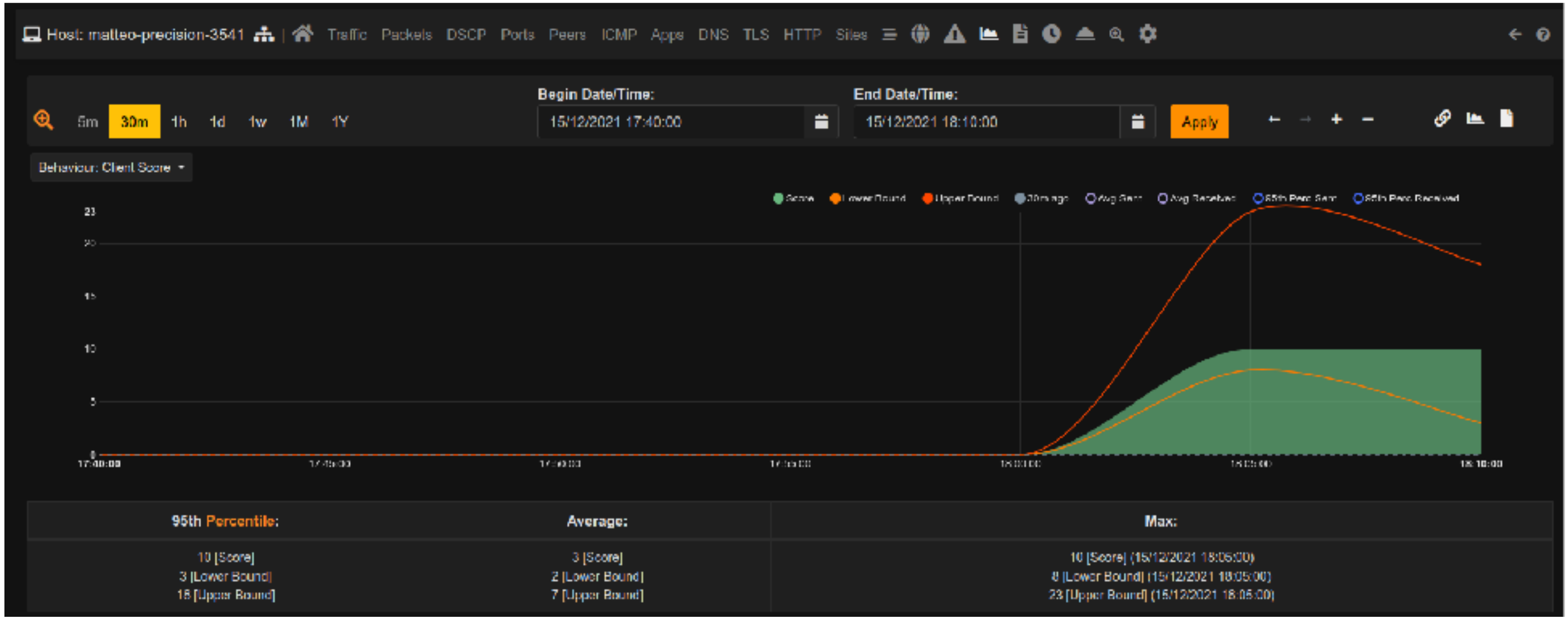
Checks and Anomaly Checks [1/2]

Introduced new checks with ntopng 5.0 and 5.1 versions

- Anomaly Checks



Checks and Anomaly Checks [2/2]

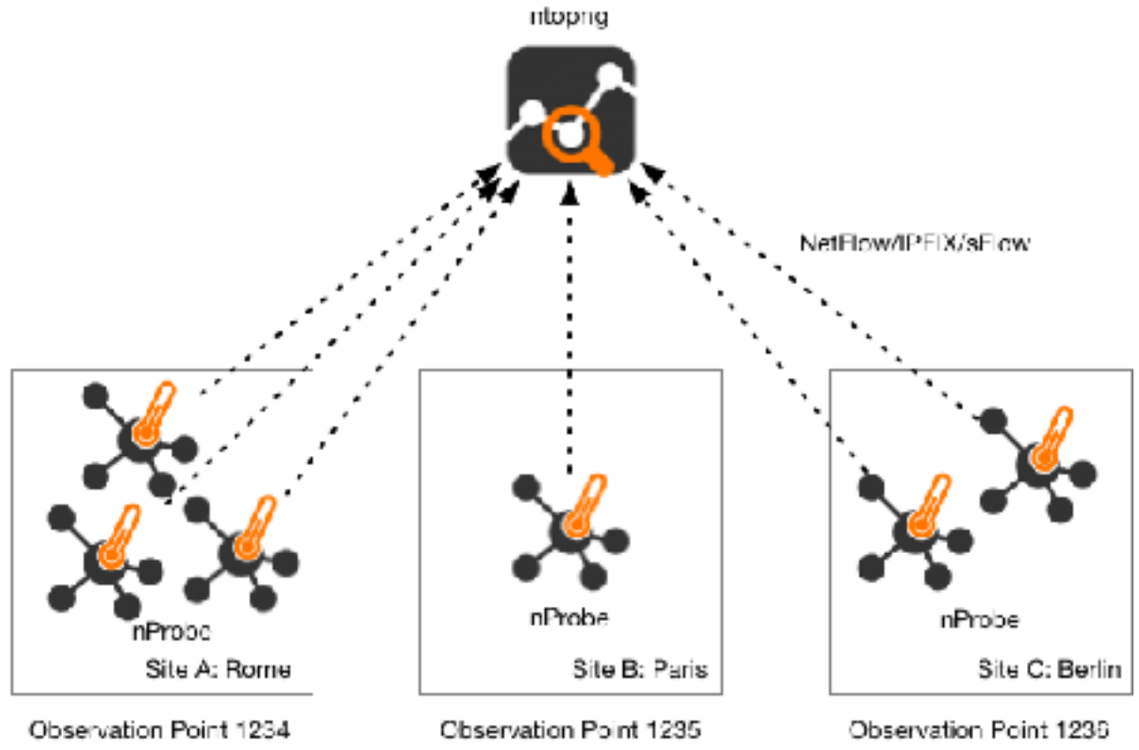


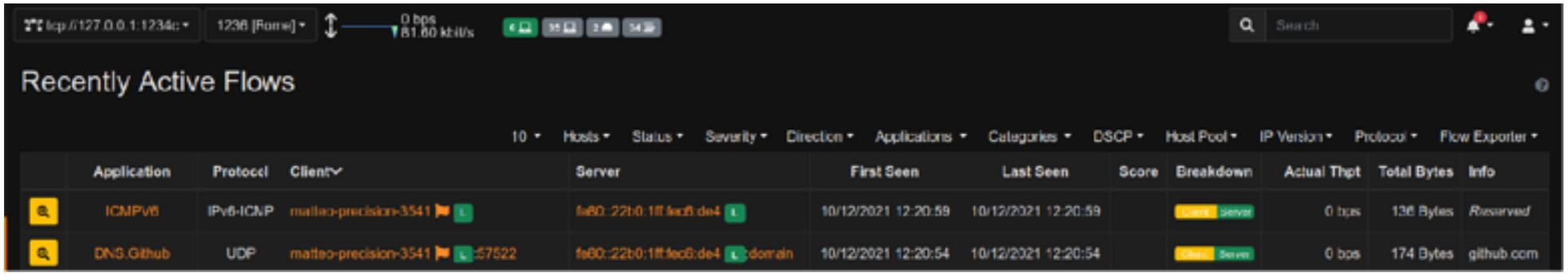
Improving Flow Visibility and Flow Analysis

Observation Points

A location in the Network where packets can be observed.

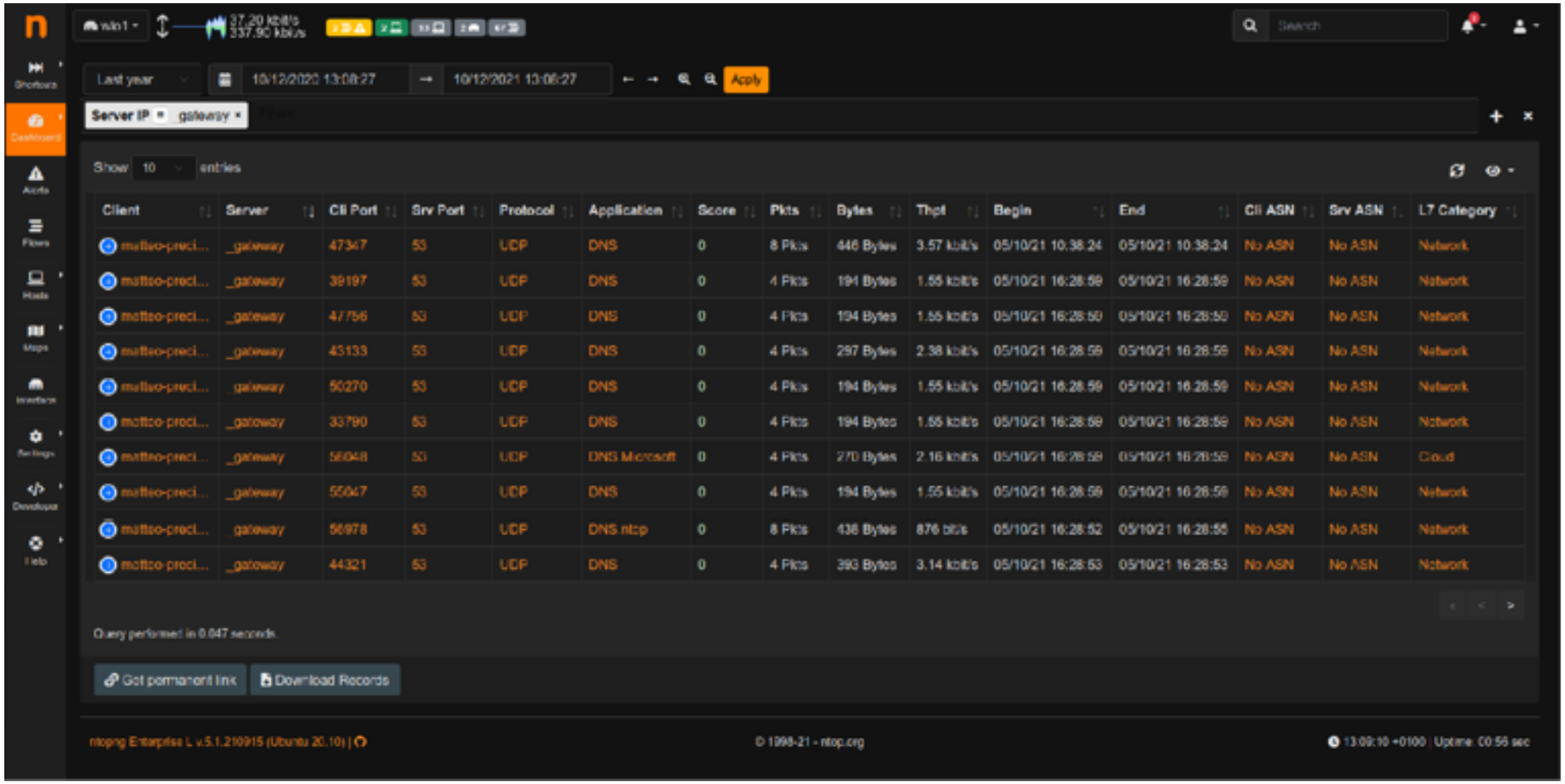
Multiple Observation points can be used per Interface.





Historical Flow Explorer

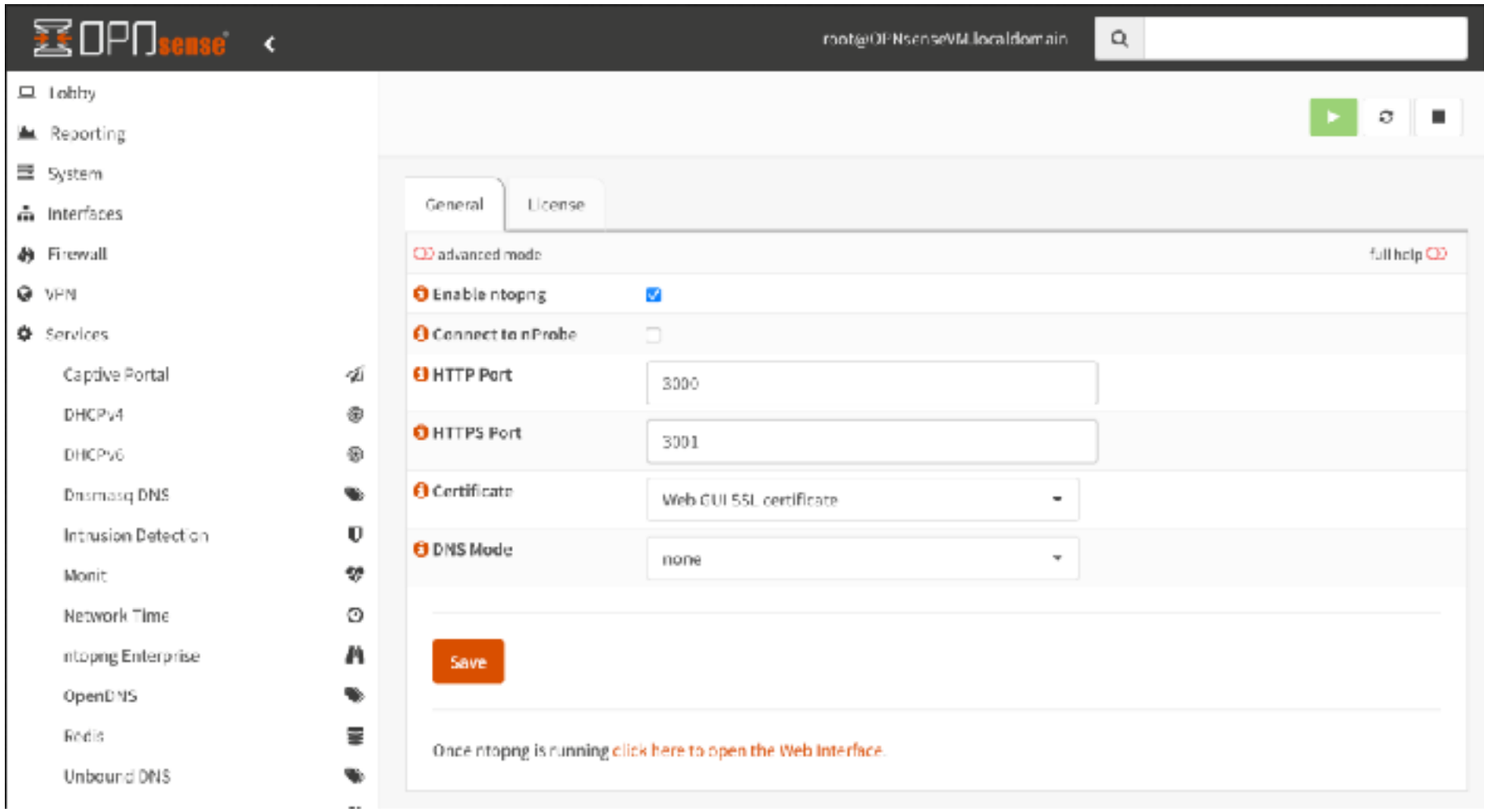
A way to visualize, filter and sort out the flows flowing through the network (feature supported by nIndex).



new Distro

Added ntopng support to 3 new distro

- pfSense
- OPNsense
- FreeBSD

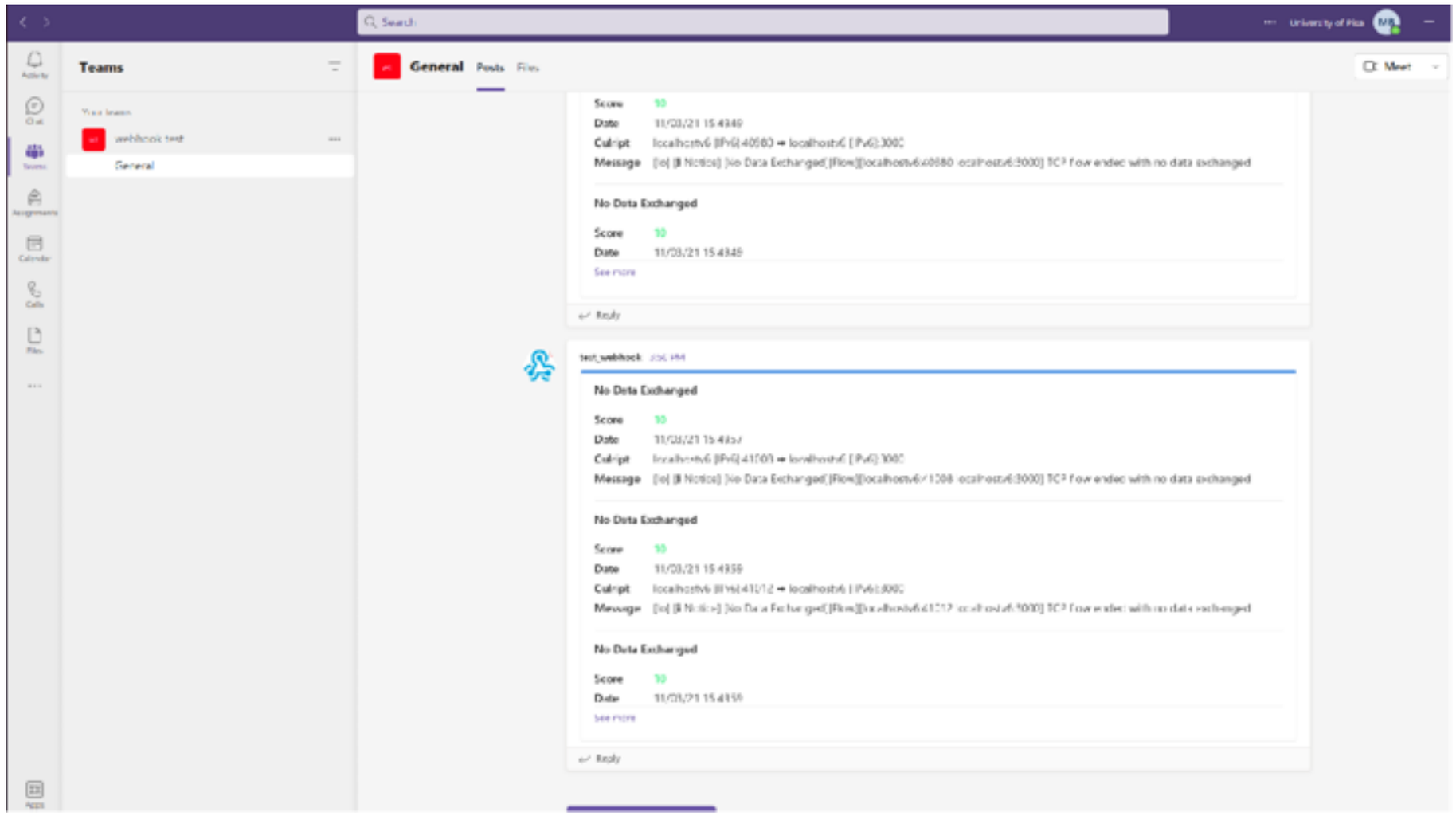


Demo

ntopng 5.1: Latest news and Updates

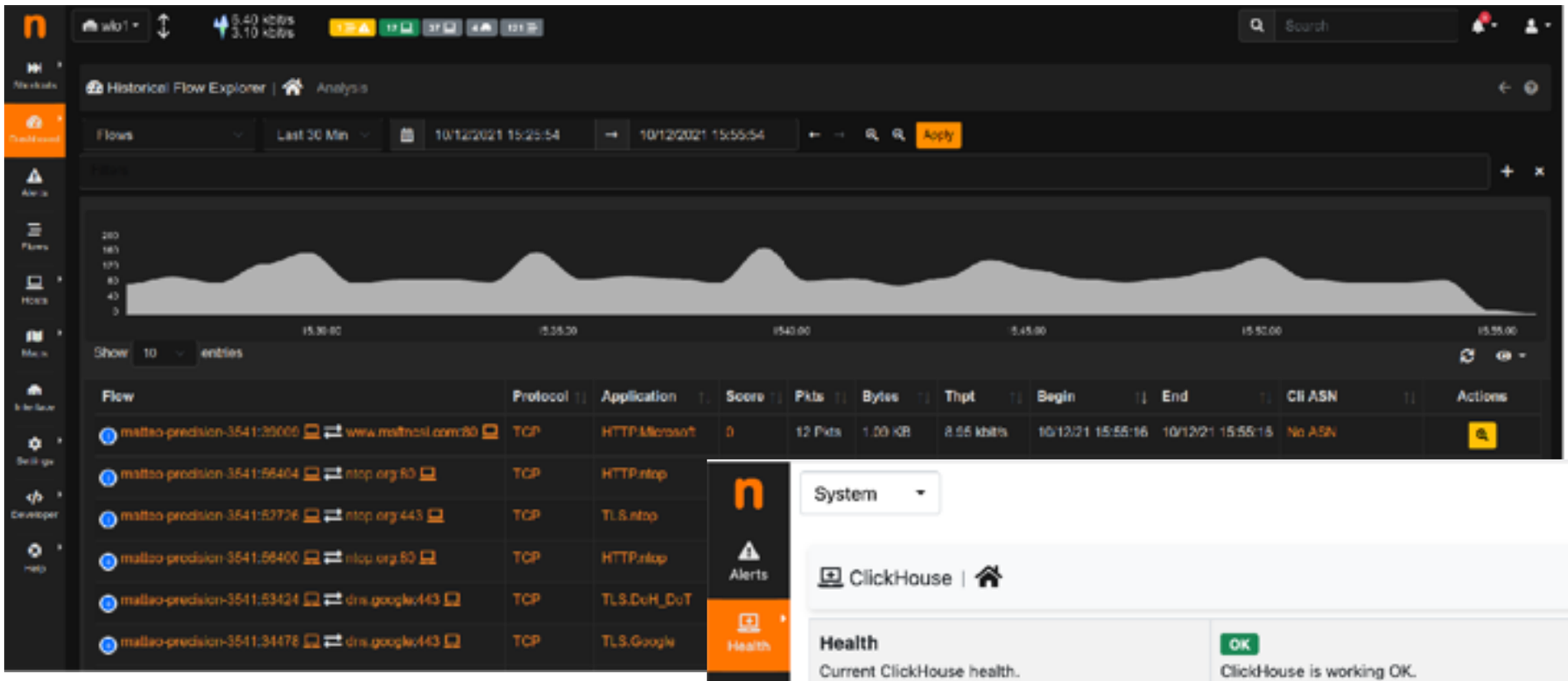
MS Teams Endpoint

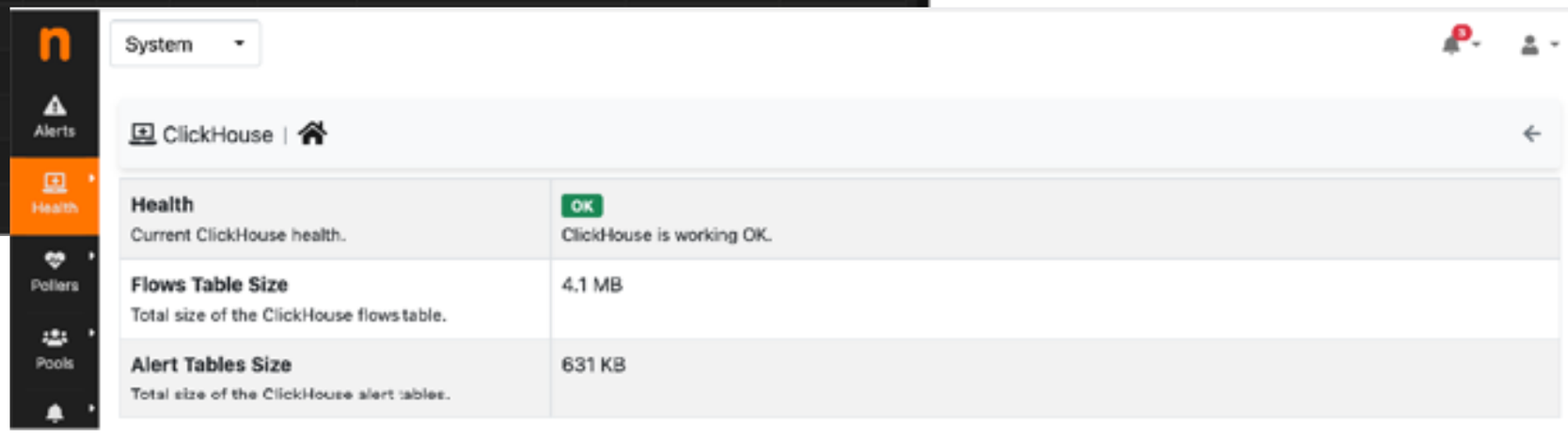
Microsoft Teams Endpoint support added.



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).



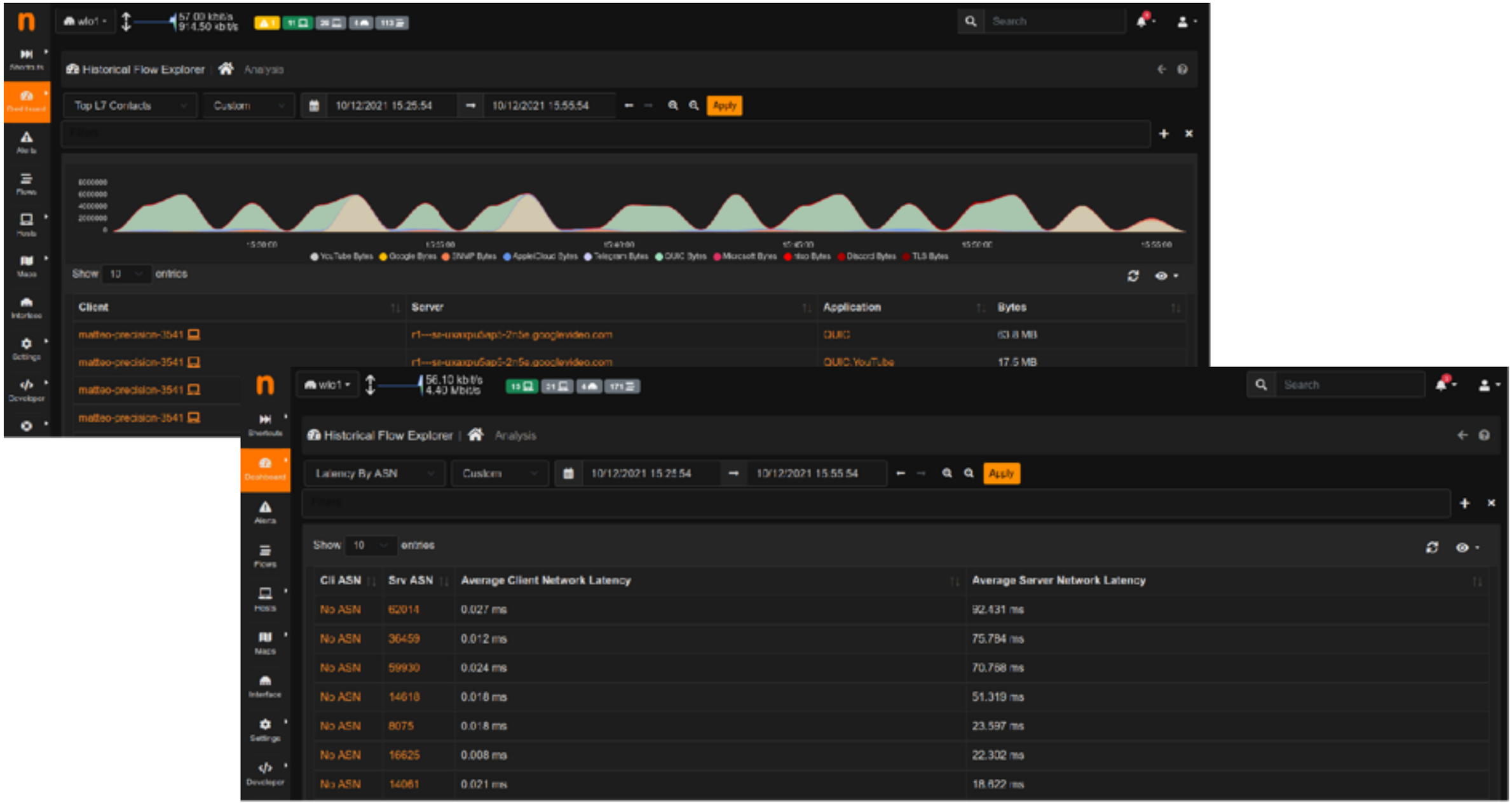


Historical Flow Explorer Revamp [1/2]

With ClickHouse introduction

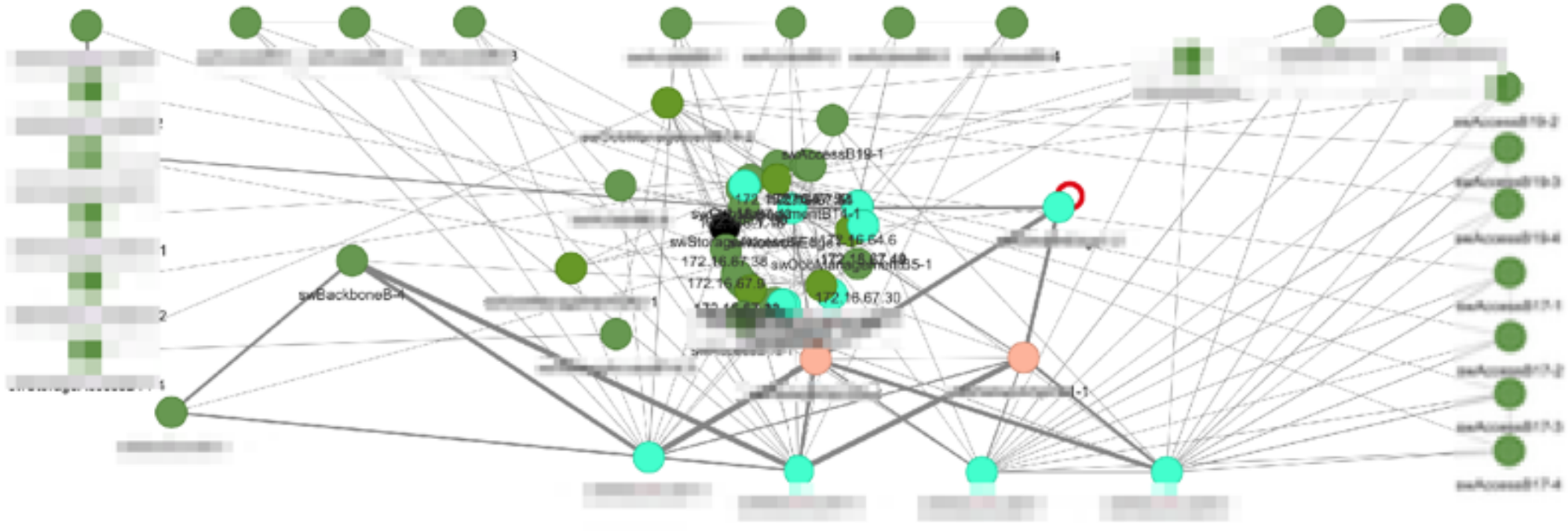
- New and more functional Historical Flow Explorer page GUI
- Support to other Queries added
  - Top L7 Contacts
  - Top Clients
  - Latency by ASN
  - …

Historical Flow Explorer Revamp [2/2]



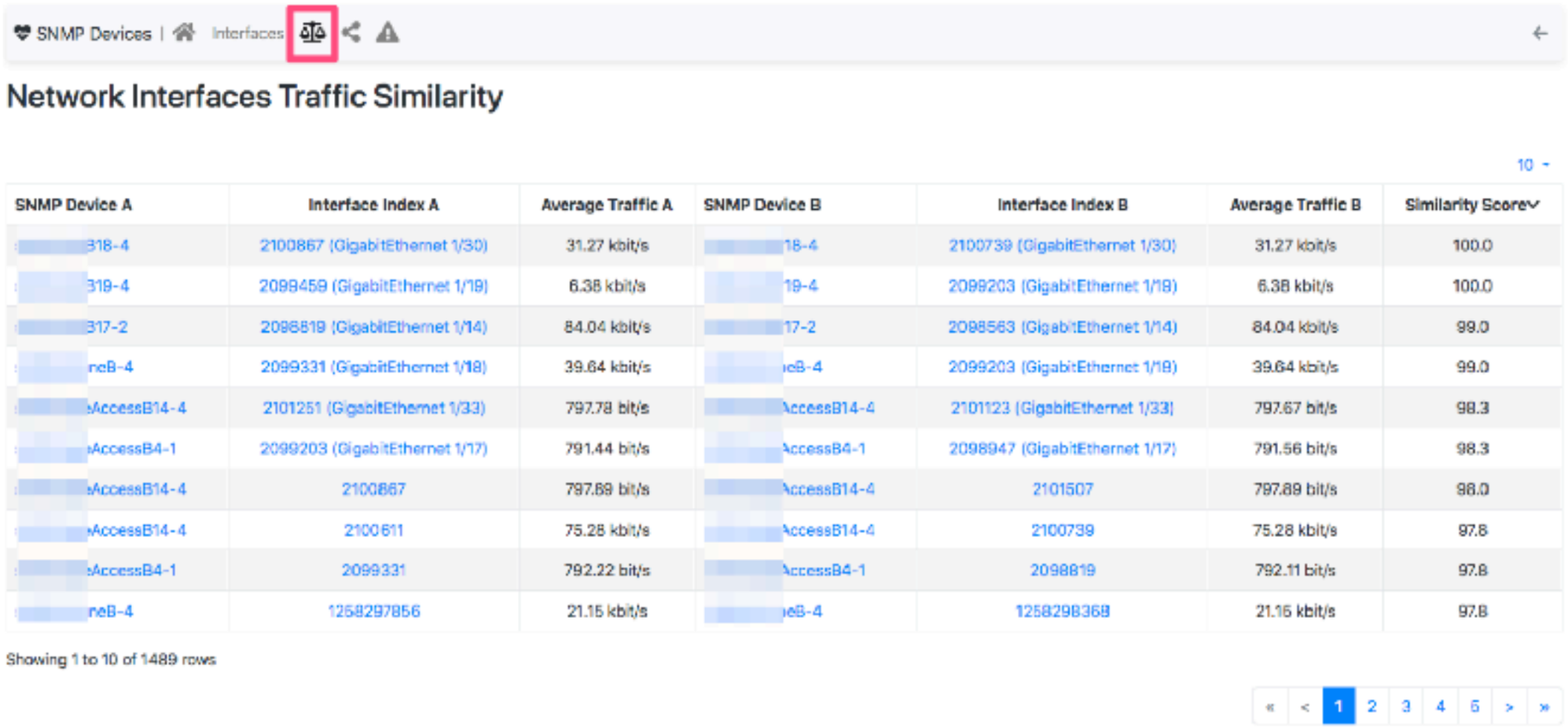
SNMP Improvements

- 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?”



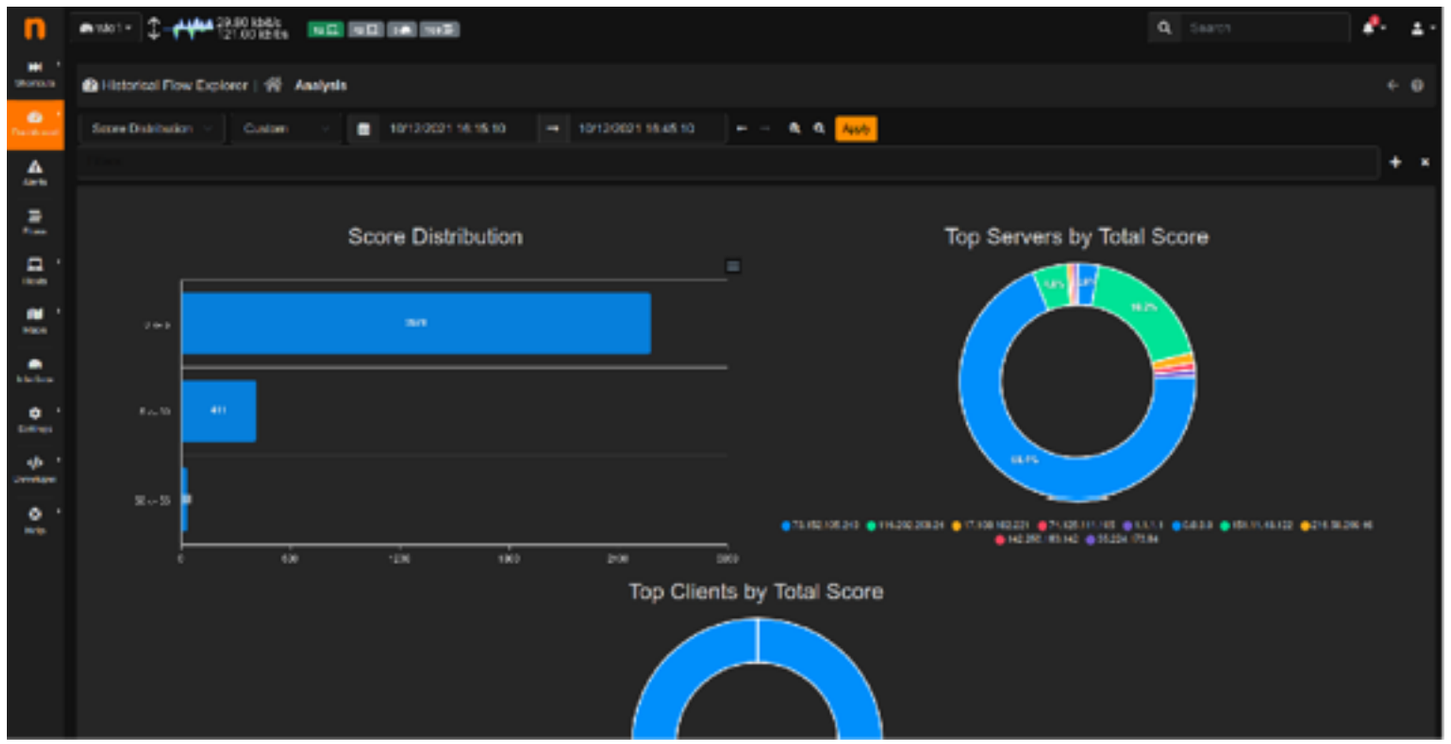
Observation Points Timeseries

- 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