

Traffic Monitoring and Enforcement for ISPs and Service Providers

Luca Deri <deri@ntop.org>
@lucaderi

Who am I

- ntop founder (<http://www.ntop.org>): company that develops open-source network security and visibility tools.
- Author of various open source software tools and contributor to popular tools (e.g. Suricata and Wireshark).
- Lecturer at the CS Dept, University of Pisa, Italy.



Presentation Overview

- This talk reports the lessons learnt while monitoring networks of various ISPs, cloud and service providers.
- Operational requirements change according to the customer so we summarise our experience.
- Most of the tools reported in this presentation are home-grown and open source whose code is available on GitHub.

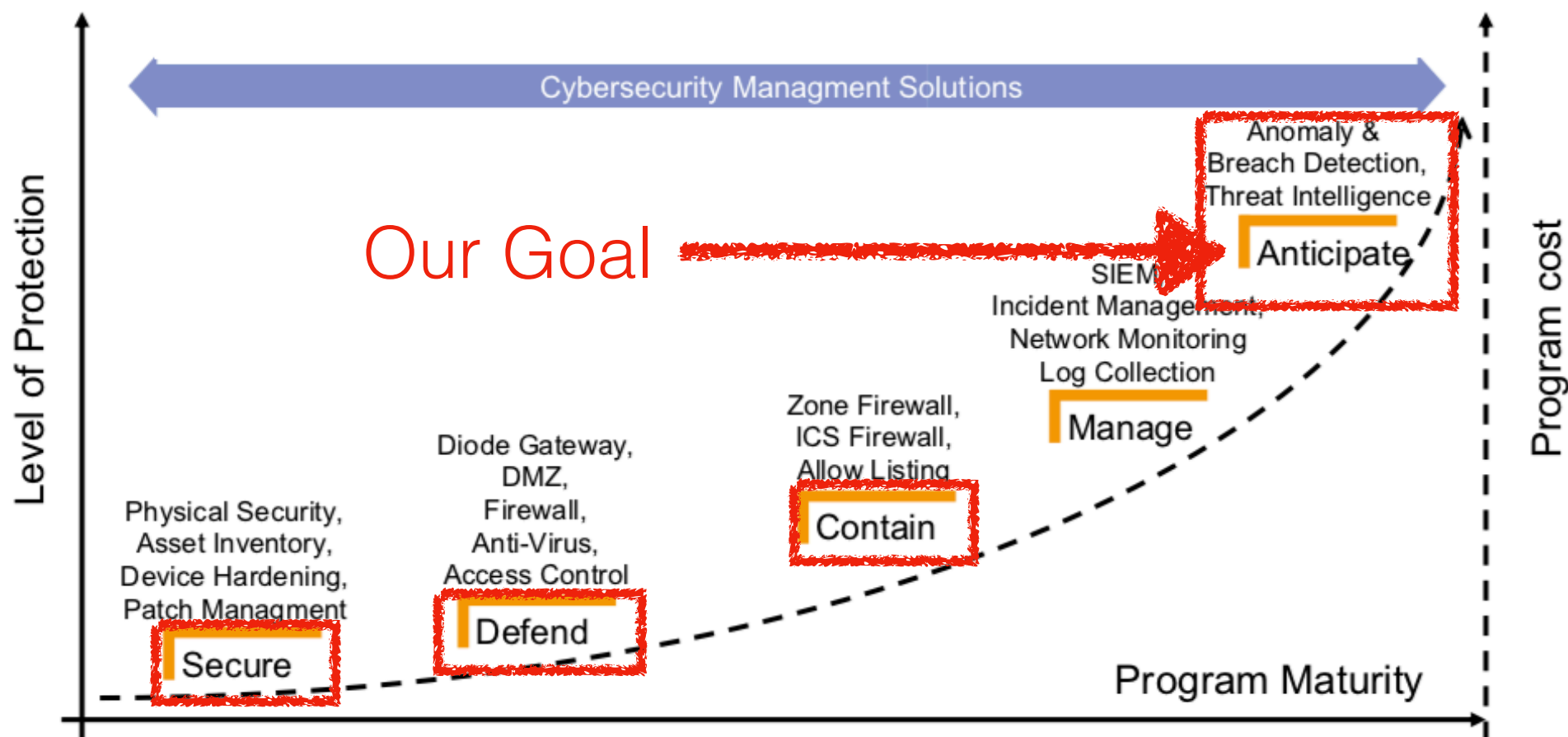
Monitoring Requirements

- Internet Service Providers
 - Prevent the network from collapsing (mostly DDoS).
 - Visibility of the main network activities in order to understand traffic flows (routing/AS-level, not host).
 - Device monitoring (interface drops, state changes).
- Service/Cloud/Hosting Providers
 - Monitor core services (e.g. DNS, email).
 - Detect severe source of troubles (e.g. heavy spammers) in order to avoid decreasing the overall network reputation.

Cybersecurity in Datacenters

- Contrary to companies where everything has to be policed, in ISPs and Providers the goal is NOT to completely cleanup traffic but keep the network infrastructure healthy by:
 - Mitigating volumetric attacks.
 - Identify and quarantine infected hosts that are potentially dangerous for the whole infrastructure.
 - Block/report suspicious activities by providing customers a detailed report in order them to address the issue.

Monitoring Goal: Anticipate



Picture courtesy of switch.ch

(D)DoS Mitigation and Detection

- All modern networks are DDoS-protected by the carriers or by leveraging on DDoS-mitigation companies.
- By nature, DDoS-mitigation is coarse, as protection mechanisms are not permanent but are enabled when specific network conditions are met.
- The outcome is that volumetric attacks not too heavy (e.g. in the 1 Gbit range, or targeting a few specific host/services) are not mitigated. This puts pressure on the infrastructure (e.g. the firewall), can block specific customers, and increase operational costs due to the need to buy more powerful equipment than necessary.

DPI at 100 Gbit [1/3]

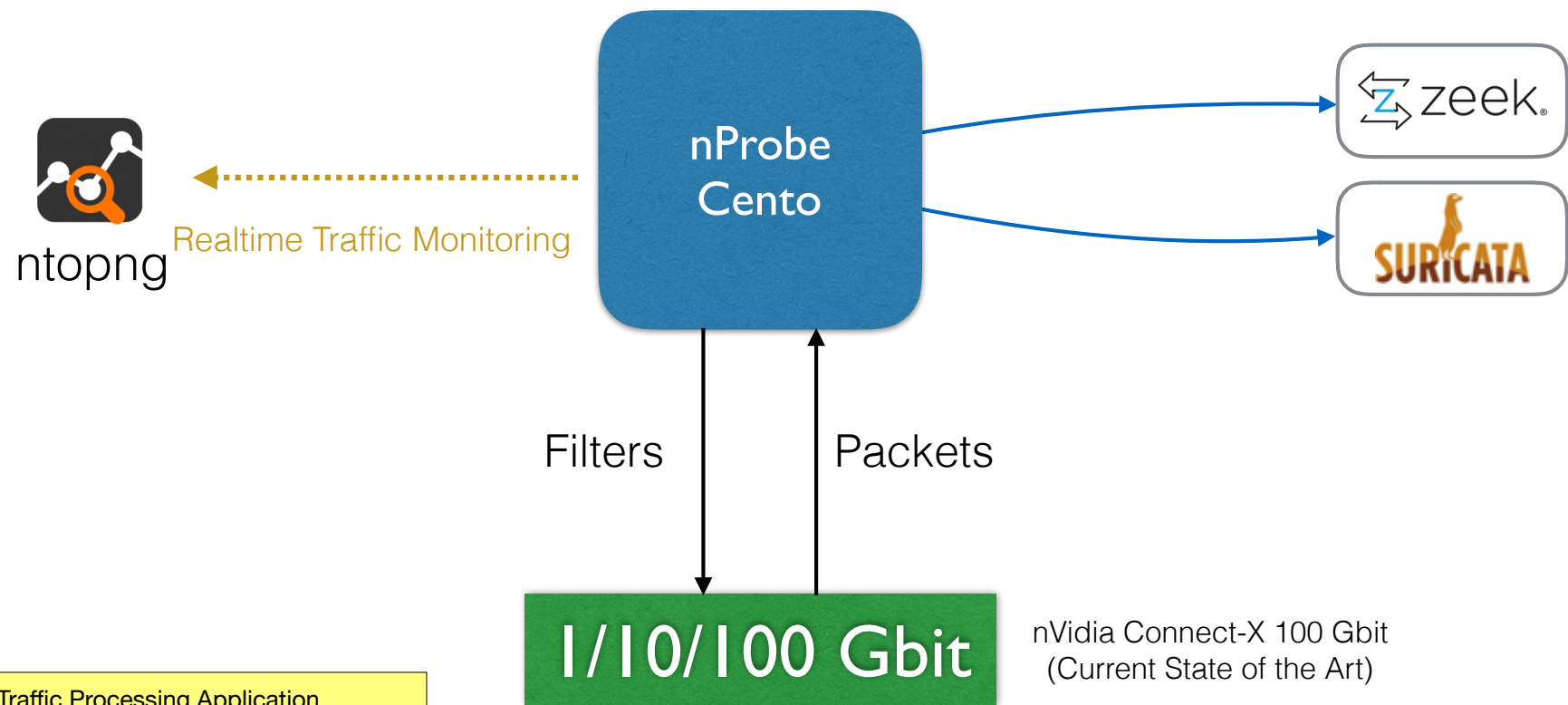
- DPI (Deep Packet Inspection) enables the inspection of packet payload in order to extract metadata and characterise traffic.
- Commercial DPI libraries are often quite expensive in price, and do not cope with high-speed (> 10 Gbit).
- Network administrators are used (often due to limitations of leading hardware manufacturers) to monitor sampled data with not DPI information.
- In 2022 we need full visibility with DPI and ETA.

DPI at 100 Gbit [2/3]

- nDPI is a GNU LGPL DPI ntop develops: 300+ protocols supported, ETA and cybersecurity traffic analysis by means of flow risk analysis.

Id	Risk	Severity	Score	CliScore	SrvScore
1	XSS Attack	Severe	250	225	25
2	SQL Injection	Severe	250	225	25
3	RCE Injection	Severe	250	225	25
4	Binary App Transfer	Severe	250	125	125
5	Known Proto on Non Std Port	Medium	50	25	25
6	Self-signed Cert	High	100	90	10
7	Obsolete TLS (v1.1 or older)	High	100	90	10
8	Weak TLS Cipher	High	100	90	10
9	TLS Cert Expired	High	100	10	90
10	TLS Cert Mismatch	High	100	50	50
11	HTTP Suspicious User-Agent	High	100	90	10
12	HTTP Numeric IP Address	Low	10	5	5
13	HTTP Suspicious URL	High	100	90	10
14	HTTP Suspicious Header	High	100	90	10
...					
39	Text With Non-Printable Chars	High	100	90	10
40	Possible Exploit	Severe	250	225	25
41	TLS Cert About To Expire	Medium	50	5	45
42	IDN Domain Name	Low	10	1	9
43	Error Code	Low	10	1	9
44	Crawler/Bot	Low	10	1	9
45	Anonymous Subscriber	Medium	50	25	25
46	Unidirectional Traffic	Low	10	5	5

DPI at 100 Gbit [3/3]



Traffic Processing Application		
nDPI	nDPI-Pro	
Packet Capture (PF_RING, DPDK)		

NOTE: When packets are not available, flow collection can also work but it will offer limited visibility due to sampling and lack of DPI

Combining Visibility with ETA

Flow: 106.75.171.61:14956 ↔ :443 | Overview

Flow Peers [Client / Server]	106.75.171.61 [40:55:39:0F:AD:C2] ↔ :443	
Protocol / Application	TCP / TLS (Malware @ Stratosphere Lab) [Confidence: DPI]	
First / Last Seen	03/09/2022 16:44:22 [02:43 ago]	03/09/2022 16:44:23 [02:42 ago]
Total Traffic	Total: 2.1 KB —	
	Client → Server: 8 Pkts / 827 Bytes —	Client ← Server: 6 Pkts / 1.3 KB —
	<div><div>106.75.171.61:14956</div><div>89.31.74.3:443</div></div>	
RTT Time Breakdown	<div>116.367 ms (client)</div>	
Client/Server Estimated Dista...	23,420 Km	14,530 Miles
Application Latency	7.0 ms	
TCP Packet Analysis	Client → Server / Client ← Server	
	Retransmissions	1 Pkts / 0 Pkts
TLS Certificate	Client Requested: 	
Max (Estimated) TCP Through...	Client → Server: 96.88 kbit/s	Client ← Server: 1.99 Mbit/s
TCP Flags	Client → Server: S A F P R	Client ← Server: S A F P
	Flow is closed.	
Total Flow Score / Score Category Breakdown	400	Cybersecurity
Issues	Description	Actions
	Blacklisted Flow [Score: 100]	
	Remote to Local Insecure Protocol [Score: 100]	
	TLS Cert. Expired [Score: 100] [07/Jun/2011 23:54:19 - 04/Jun/2021 23:54:19] ?	
	Unsafe TLS Ciphers [Score: 100] [Cipher TLS_RSA_WITH_AES_128_CBC_SHA] ?	

Analysing Traffic Behaviour

⚙ Behavioural Checks | All **Host** Interface Local Networks SNMP Flow System Syslog

All (20) Enabled (3) Disabled (17)

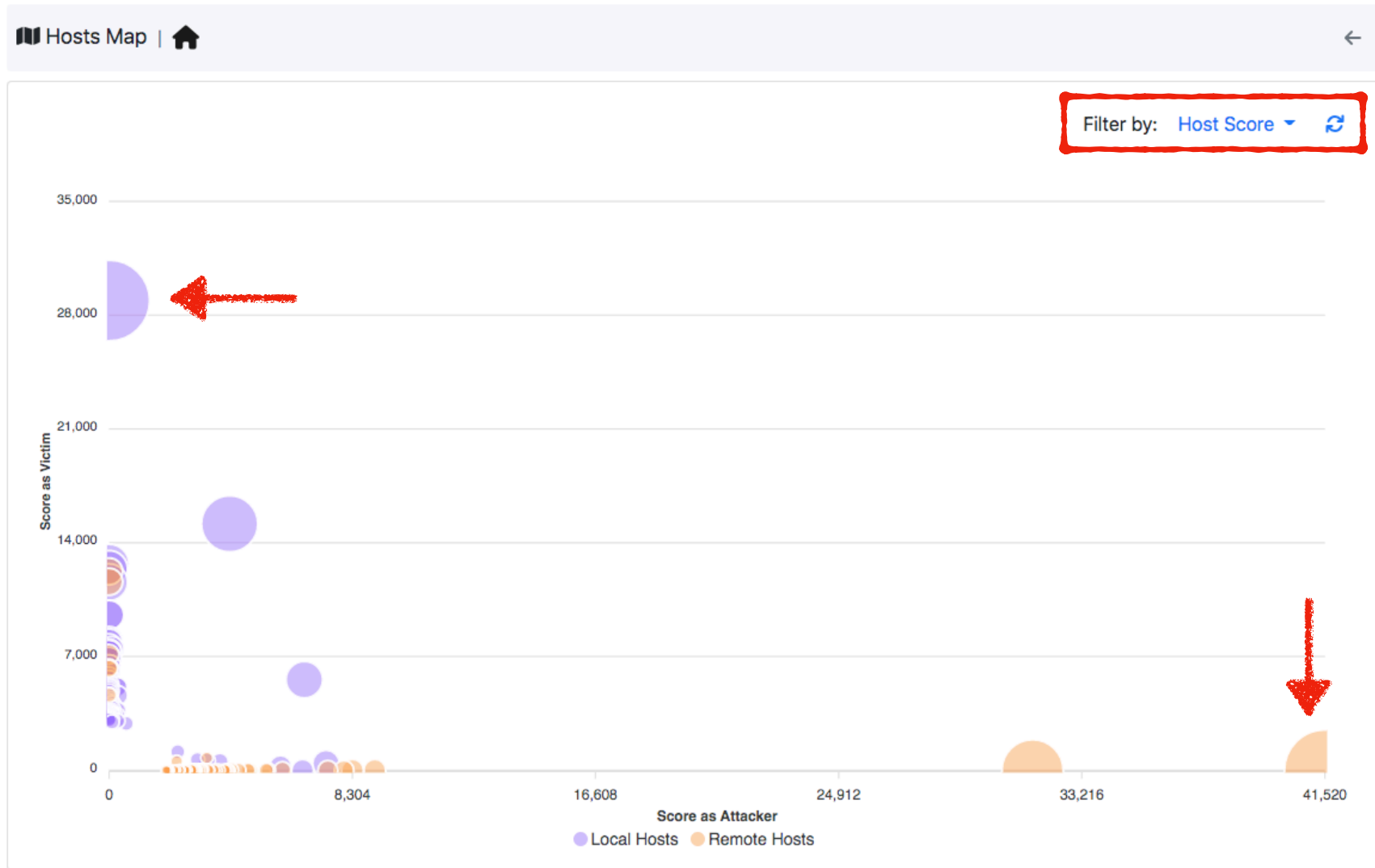
Filter Categories Search Script:

Name	Interface	Category	Description	Values	Action
Countries Contacts Alert			Trigger an alert when the number of different countries contacted exceeds the threshold	> 100 Contacts (Minute)	
Dangerous Host			Triggers an alert and adds the host to the jailed hosts pool for 30 minutes, when the configured score threshold is cros...	> 1000 Score (Minute)	
DNS Server Contacts Alert			Trigger an alert when the number of different DNS servers contacted exceeds the threshold	> 5 Contacts (Minute)	
DNS Traffic Alert			Trigger an alert when layer 2 Bytes delta (sent + received) for DNS traffic exceeds the threshold	> (1 MB)	
Domain Names Contacts Alert			Trigger an alert when the number of contacted Domain Names is greater then a certain threshold	> 250 Contacts (Minute)	
FIN Scan Alert			Trigger an alert when the number of sent/received FINs/min (with no response) exceeds the threshold	> 256 FINs/min (Minute)	
Flow Flood Alert			Trigger an alert when the new client/server Flows/sec exceeds the threshold	> 256 Flows/sec (Minute)	
Flows Anomaly			Detects anomalies in active flows number		
ICMP Flood Alert			Trigger an alert when the number of sent/received ICMP Flows/sec exceeds the threshold	> 256 ICMP Flows/sec (Minute)	
NTP Server Contacts Alert			Trigger an alert when the number of different NTP servers contacted exceeds the threshold	> 5 Contacts (Minute)	

Showing 1 to 10 of 20 rows

« < 1 2 > »

Spotting Issues [1/3]

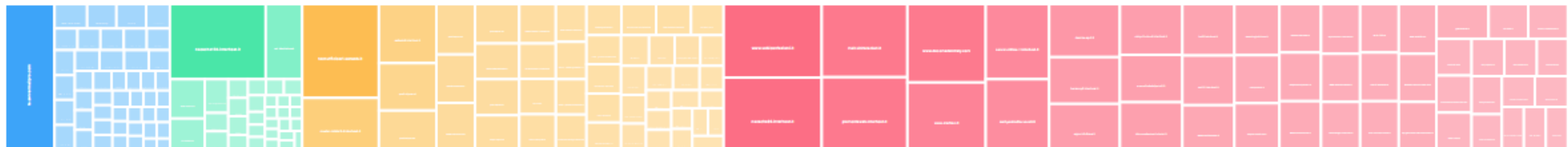


Spotting Issues [2/3]

Networks



Networks Score



10 ▾

Network Name	Chart	Hosts	Score	Alerted Flows	Breakdown	Throughput	Traffic
89.1.1.0/21		1435	465,051	0	<div><div>Sent</div><div>Rcvd</div></div>	952.95 Mbit/s	361.04 GB
194.1.1.0/24		138	55,497	0	<div><div>Sent</div><div>Rcvd</div></div>	38.88 Mbit/s	38.73 GB
185.1.1.0/22		112	12,752	0	<div><div>Rcvd</div></div>	512.12 kbit/s	44.63 GB
151.1.1.0/22		788	293,628	0	<div><div>Sent</div><div>Rcvd</div></div>	1.06 Gbit/s	381.67 GB

Showing 1 to 4 of 4 rows



Spotting Issues [3/3]

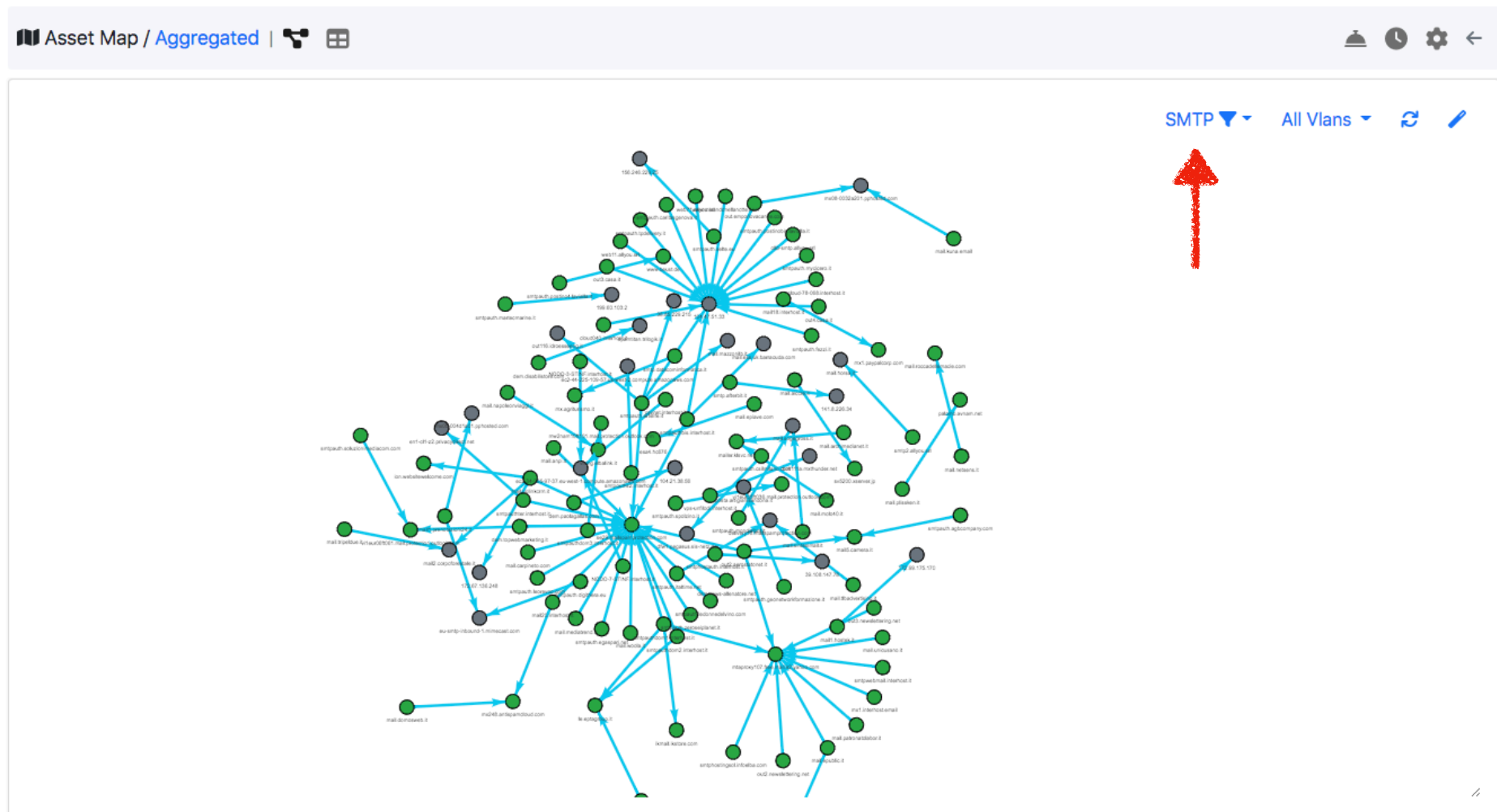
Autonomous Systems



AS number	Hosts	Name	Seen Since	Score▼	Alerted Flows	Breakdown	Throughput	Traffic
24994	2507	genesys informatica srl	08:54:25	795,686		<div><div>Sent</div><div>Rcvd</div></div>	451.62 Mbit/s	2.22 TB
30722	2260	Vodafone Italia S.p.A.	08:54:25	120,452		<div><div>Sent</div><div>Rcvd</div></div>	33.65 Mbit/s	249.81 GB
3269	3053	Telecom Italia S.p.A.	08:54:25	98,442		<div><div>Se</div><div>Rcvd</div></div>	37.97 Mbit/s	234.94 GB
12874	1439	Fastweb SpA	08:54:25	62,909		<div><div>Se</div><div>Rcvd</div></div>	39.0 Mbit/s	229.01 GB
16276	878	OVH SAS	08:54:25	49,774		<div><div>Sent</div><div>Rcvd</div></div>	26.17 Mbit/s	47.51 GB
1267	1733	WIND TRE S.P.A.	08:54:25	27,540		<div><div>Se</div><div>Rcvd</div></div>	48.83 Mbit/s	130.83 GB
5602	103	IRIDEOS S.P.A.	08:54:25	24,701		<div><div>Sent</div><div>Rcvd</div></div>	120.76 kbit/s	16.94 GB
15169	3806	Google LLC	08:54:25	26,332		<div><div>Sen</div><div>Rcvd</div></div>	8.39 Mbit/s	58.76 GB
13335	4262	Cloudflare, Inc.	08:54:25	22,851		<div><div>Sent</div><div>Rcvd</div></div>	12.64 Mbit/s	47.56 GB
398324	126	Censys, Inc.	08:54:25	20,156		<div><div>Sent</div><div>Rcvd</div></div>	45.04 kbit/s	50.53 MB

Showing 1 to 10 of 2729 rows

Know Your Network [1/2]



Know Your Network [2/2]

Asset Map / Aggregated

Standard View Centrality View

Show 10 entries

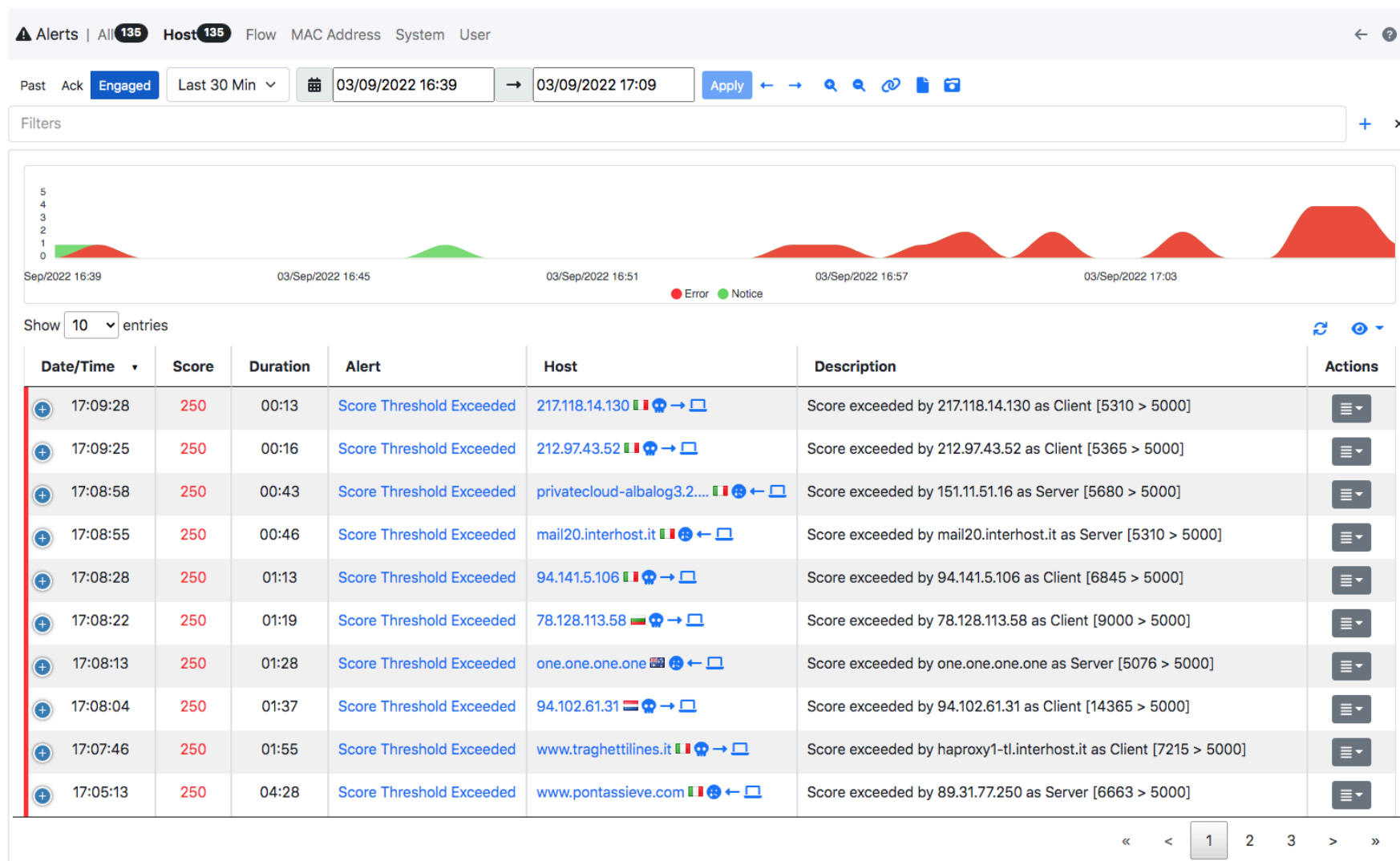
NTP Search:

Host	Total Edges	Incoming Edges	Outgoing Edges
ntp1.interhost.it [194.242.61.99]	1494	747	747
pugot.canonical.com [91.189.94.4]	156	78	78
124.65.30.80	146	73	73
ntp2.inrim.it [193.204.114.233]	128	64	64
time.cloudflare.com [162.159.200.1]	100	50	50
ntp72.kashra-server.com [135.125.165.133]	100	50	50
server1.quickdrivingtestcancellations.net [85.199.214.99]	94	47	47
ntp74.kashra-server.com [135.125.165.135]	92	46	46
ntp12.kashra-server.com [51.38.27.129]	82	41	41
ntp25.kashra-server.com [51.195.1.216]	82	41	41

Showing 1 to 10 of 388 entries

« < 1 2 3 4 5 ... 39 > »

From Alerts to Actions [1/2]



From Alerts to Actions [2/2]

Add New Endpoint [X]

Name

Type

- ✓ Discord
- Elasticsearch
- Email
- Fail2Ban**
- Shell Script**
- Slack
- Syslog**
- Microsoft Teams
- Telegram
- Webhook**

WebHook URL

Instructions:

- Open the Discord channel
- From the channel menu,
- Click on Webhooks menu
- Click the Create Webhook button (it on the ntopng recipients page)
- Note the URL from the WebHook URL field to be copied in the field above.
- Click the Save button.

post the messages (note that you can set

Add

Final Remarks

- Over the past 20+ years ntop created open source software framework for efficiently monitoring traffic.
- Commodity hardware, with adequate software, can now match the performance and flexibility that modern network operators require.



Many thanks to Hosting Solutions for supporting this work !

