Traffic Monitoring and Enforcement for ISPs and Service Providers

Luca Deri <deri@ntop.org>
@lucaderi

ntop

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 talks 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.
- Tools reported in this presentation are home-grown and open source whose code is available on GitHub.

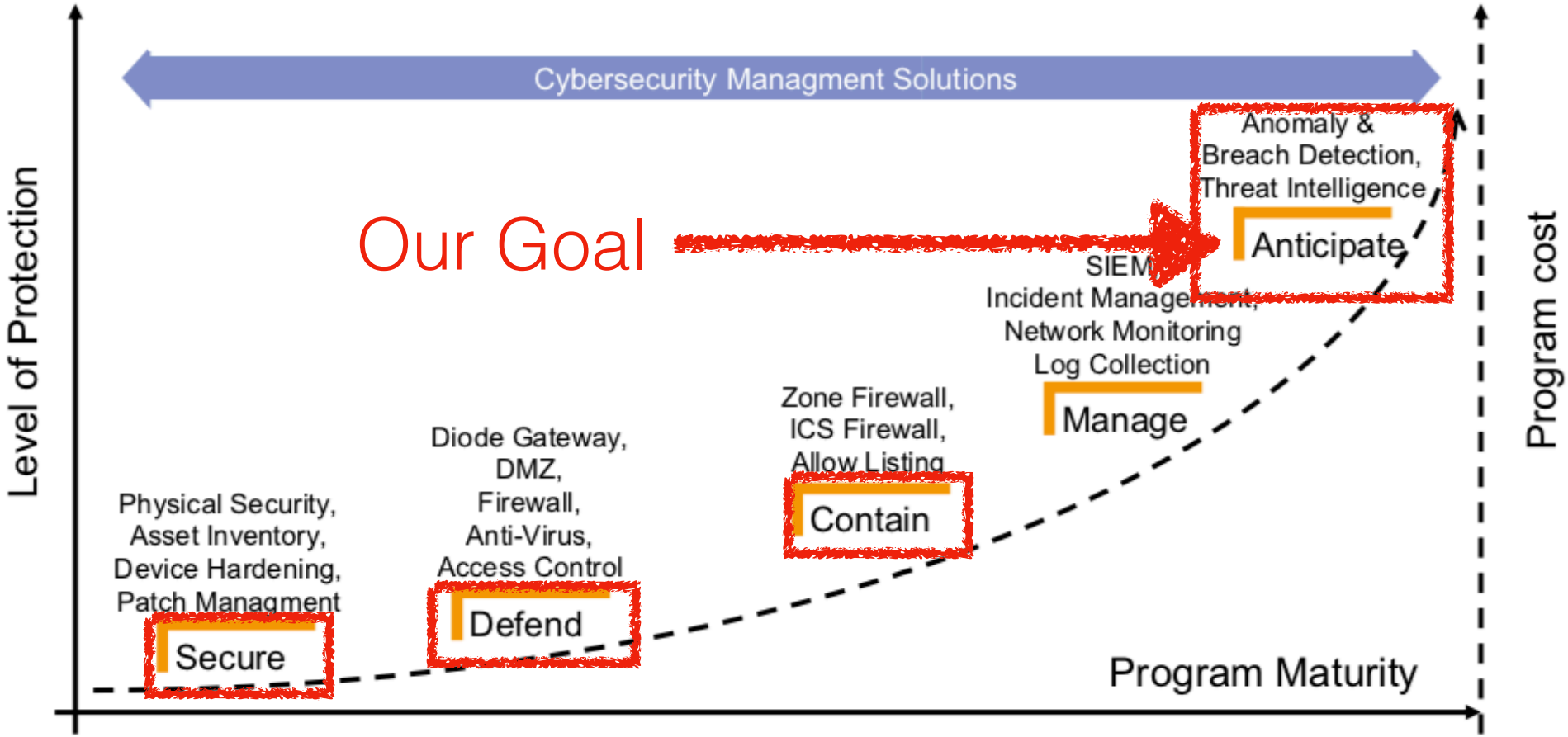
Monitoring Requirements

- 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 and 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]

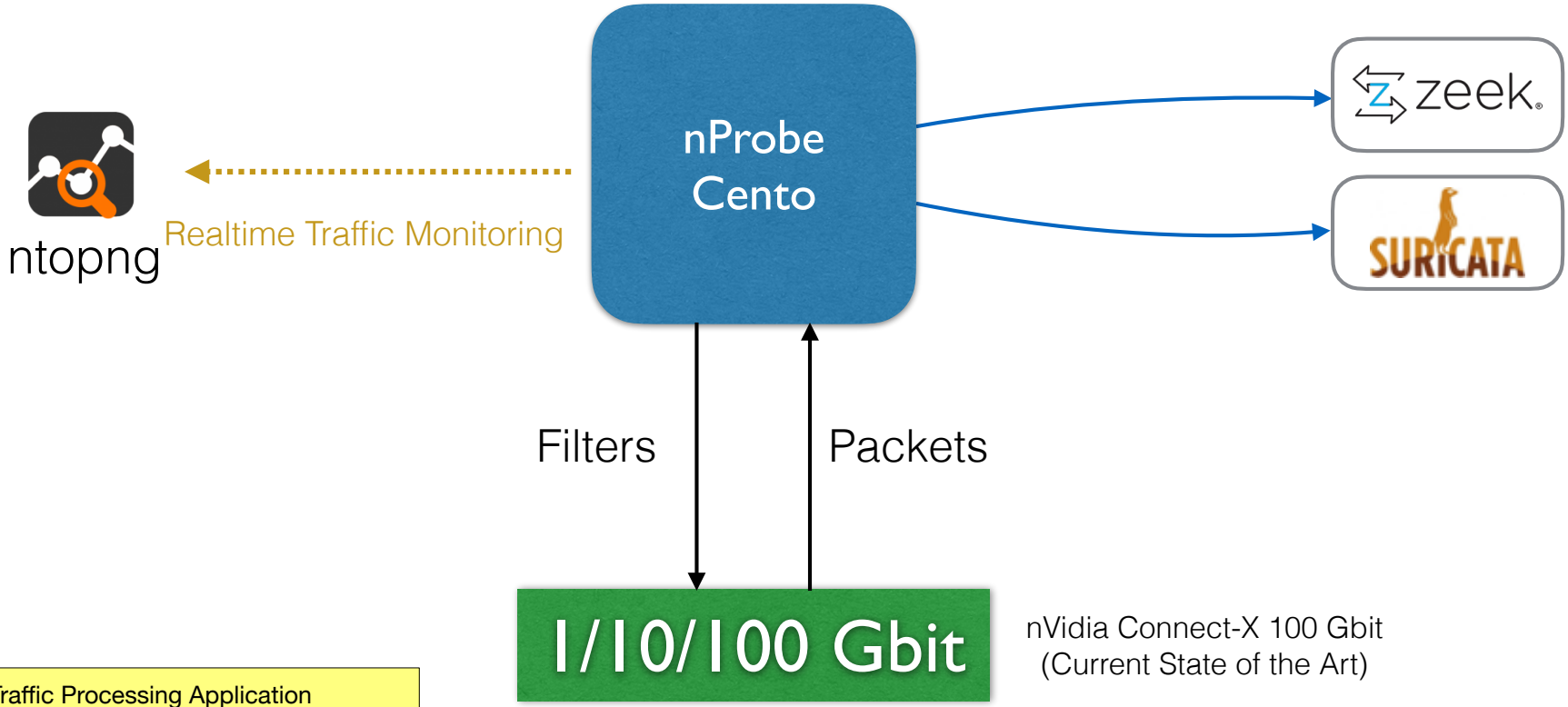
- DPI (Deep Packet Inspection) enables the inspection of packet payload in order to extract metadata and characterise traffic.
- Commercial DPI libraries are often quite expensive in price, and do not cope with high-speed (> 10 Gbit).
- Network administrators are used (often due to limitations of leading hardware manufacturers) to monitor sampled data with not DPI information.
- In 2024 we need full visibility with DPI and ETA.

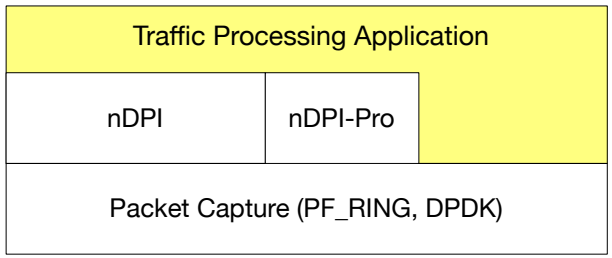
DPI at 100 Gbit [2/3]

- nDPI is a GNU LGPL DPI ntop develops: 430+ 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

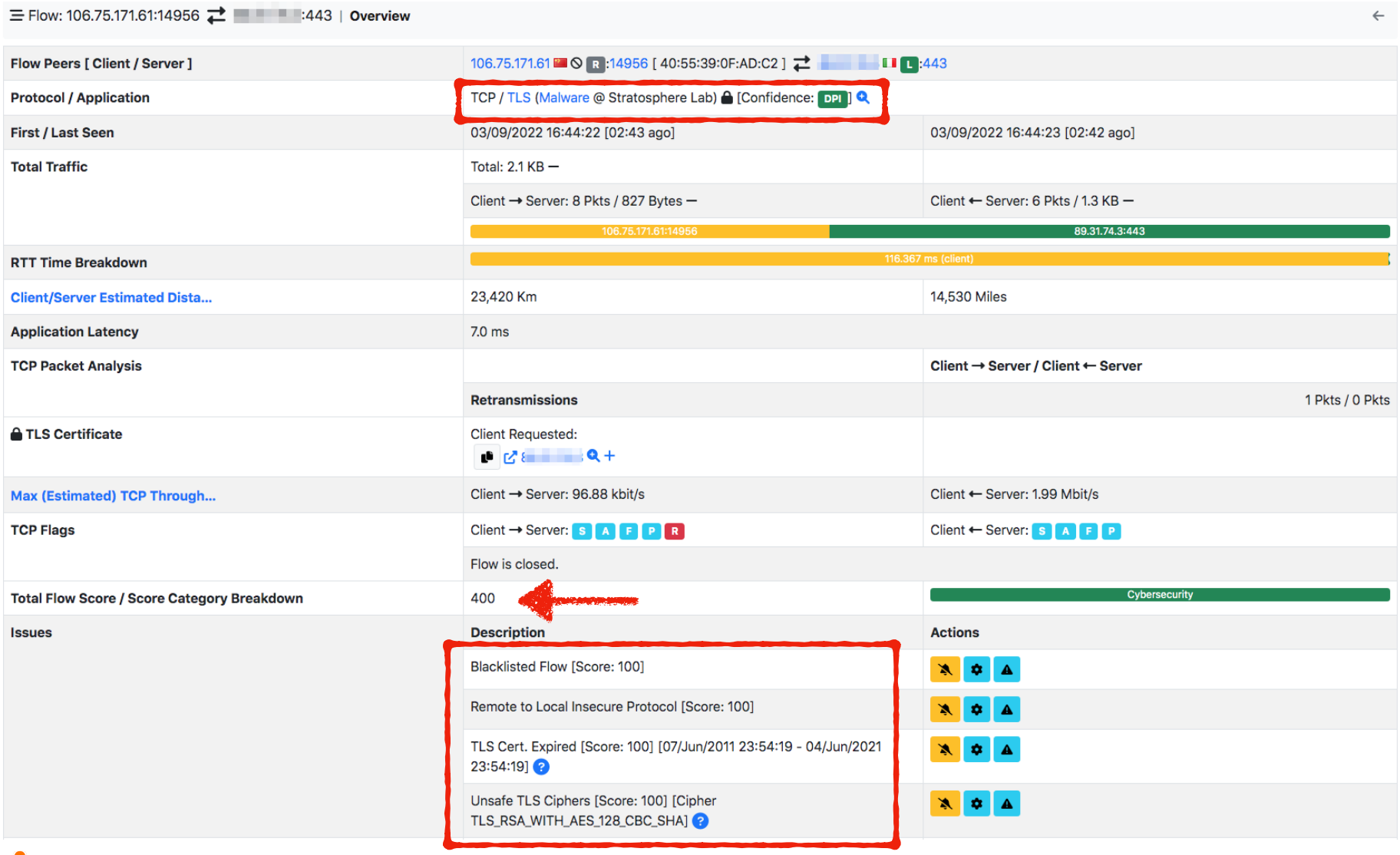
DPI at 100 Gbit [3/3]





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



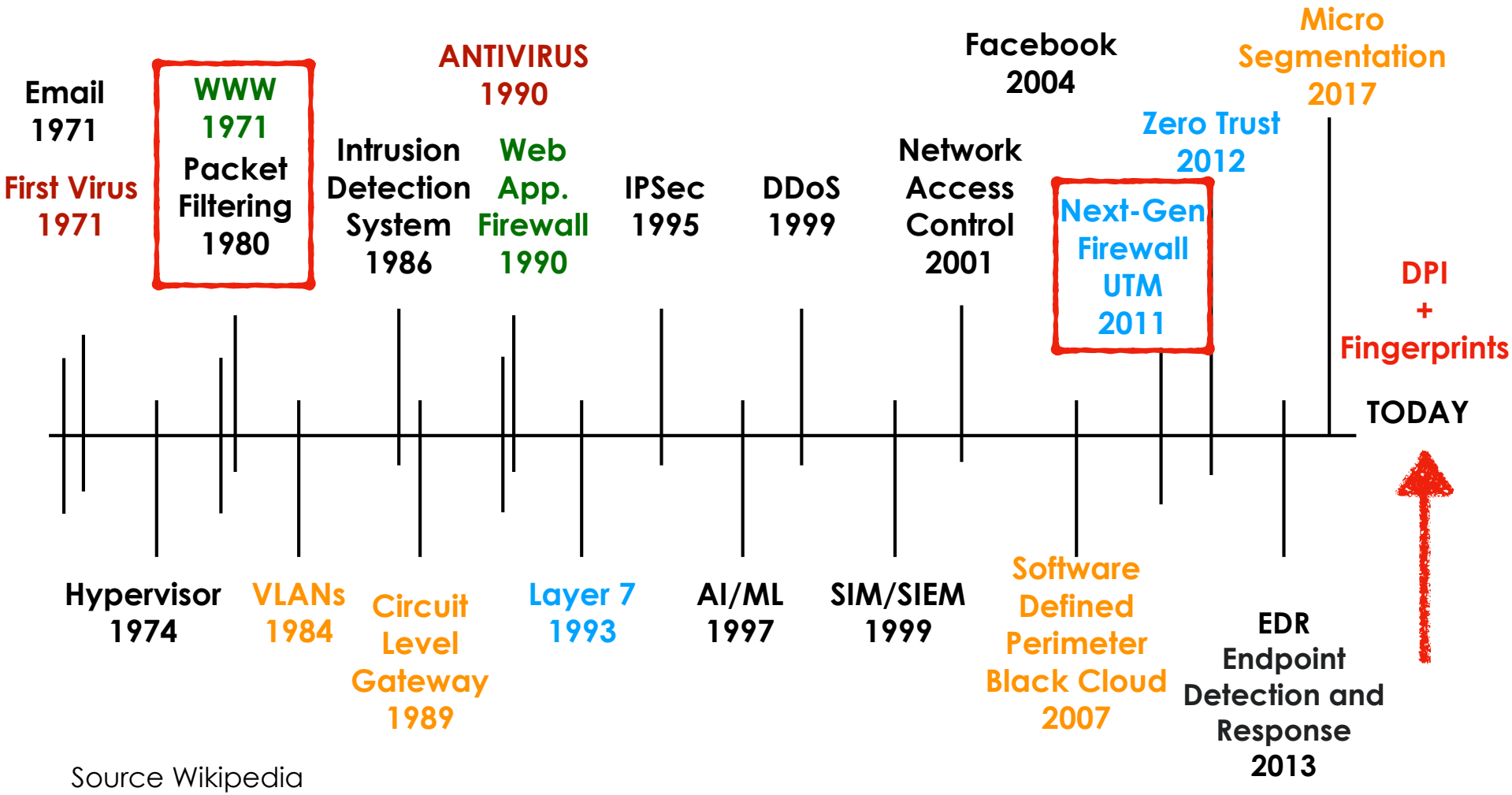
Anticipate Problems [1/4]

- Firewalls evolved:
  - IP-header based rules (ACL) - 1980
  - Next-generation Firewalls (L7 protocol) - 2011
- Traffic fingerprinting refers to the process of identifying and gathering specific information about a system or network to create a (in theory) unique profile or “fingerprint”.
- As fingerprints are created on the initial few traffic bytes, blocking malicious fingerprints means that we can stop threats before they hit the network.

Anticipate Problems [2/4]

- Supported Fingerprints
  - (Anonymous) VPNs (e.g. OpenVPN)
  - Malicious QUIC/TLS applications
  - SSH-based Bots
  - Outdated/unwanted devices (DHCP)
  - Unknown and Encrypted Protocols
  - Cryptominers

Anticipate Problems [3/4]



Source Wikipedia

Anticipate Problems [4/4]

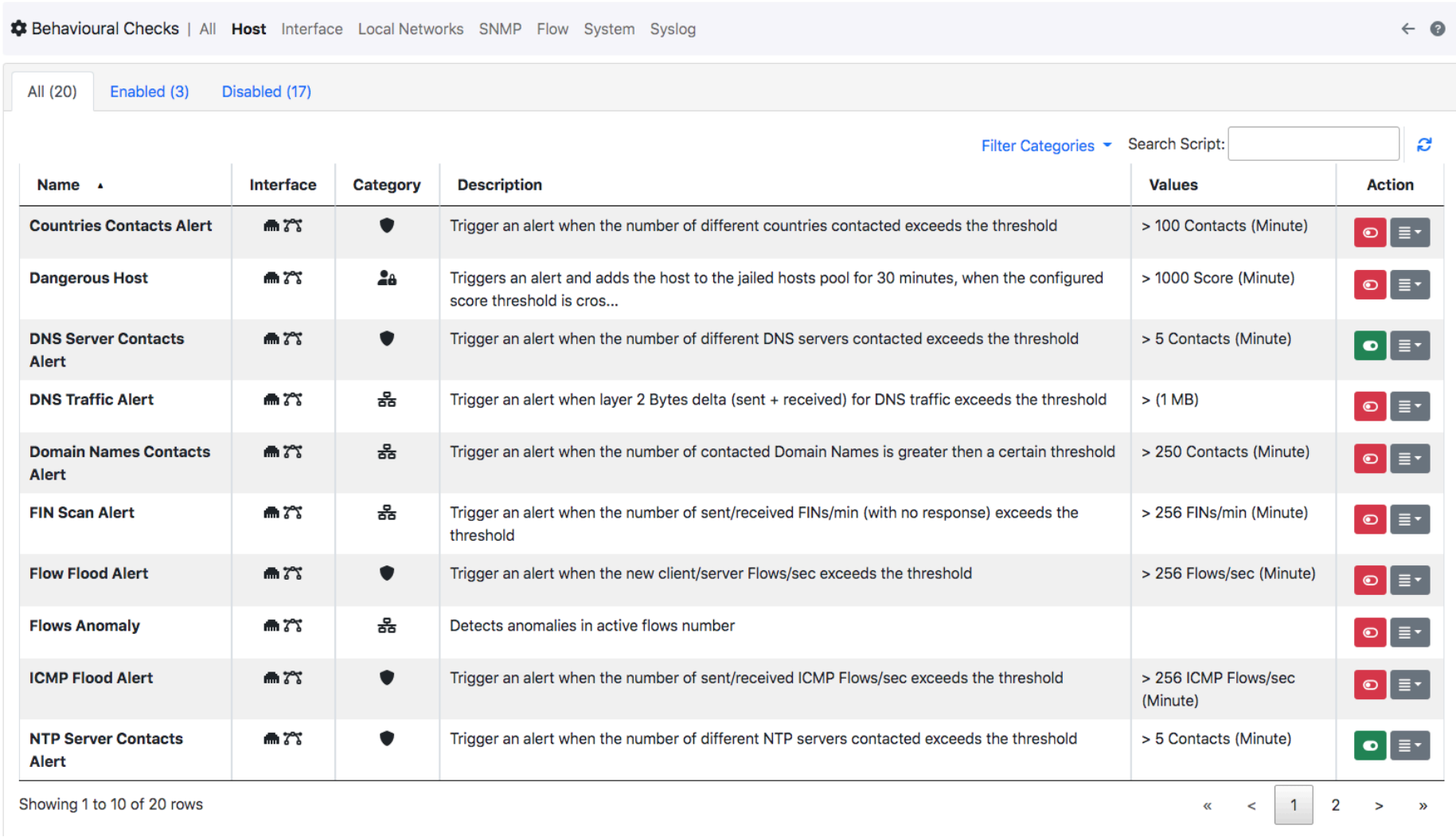
```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480
Ethernet II, Src: 76:ac:b9:35:30:da (76:ac:b9:35:30:da), Dst:
Internet Protocol Version 4, Src: 192.168.10.145 (192.168.10.
Transmission Control Protocol, Src Port: 49175, Dst Port: 888
    Source Port: 49175
    Destination Port: 8888
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 253744456
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x002 (SYN)
    Window: 65535
    [Calculated window size: 65535]
    Checksum: 0x5297 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

https://zmap.io/

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (48
Ethernet II, Src: 76:ac:b9:35:30:da (76:ac:b9:35:30:da), Ds
Internet Protocol Version 4, Src: 192.168.10.145 (192.168.1
Transmission Control Protocol, Src Port: 46998, Dst Port: 8
    Source Port: 46998
    Destination Port: 8888
    [Stream index: 0]
    [Stream Packet Number: 1]
  > [Conversation completeness: Incomplete (35)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1163206847
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x002 (SYN)
    Window: 1024
    [Calculated window size: 1024]
    Checksum: 0xd56b [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
```

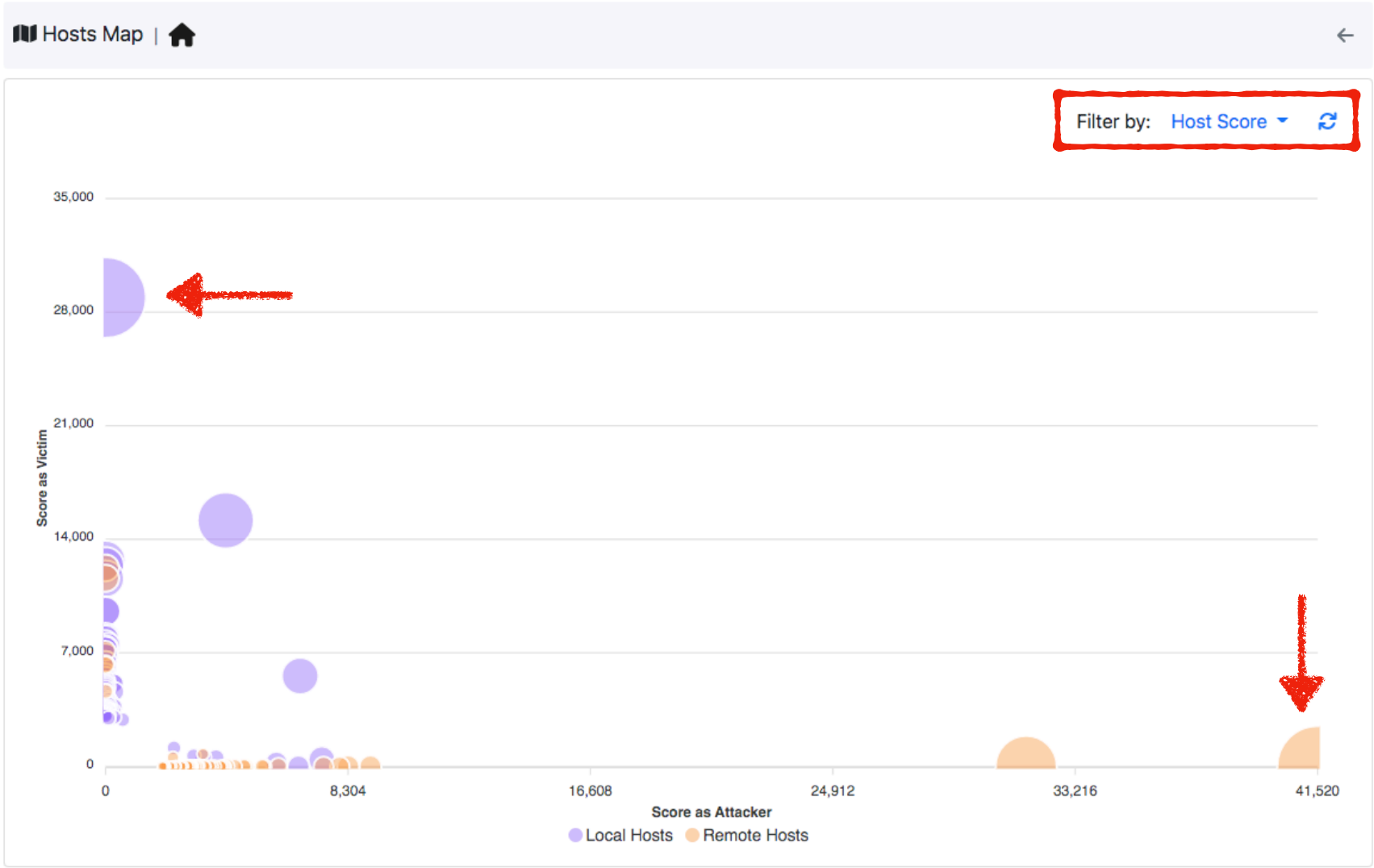
https://github.com/robertdavidgraham/masscan

Analysing Traffic Behaviour



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)	

Spotting Issues [1/3]



Spotting Issues [2/3]

Networks

Networks Score

10

Network Name	Chart	Hosts	Score	Alerted Flows	Breakdown	Throughput	Traffic
89.[redacted]/21		1435	465,051	0	Sent Rcvd	952.95 Mbit/s	361.04 GB
194.[redacted]/24		138	55,497	0	Sent Rcvd	38.88 Mbit/s	38.73 GB
185.[redacted]/22		112	12,752	0	Rcvd	512.12 kbit/s	44.63 GB
151.[redacted]/22		788	293,628	0	Sent Rcvd	1.06 Gbit/s	381.67 GB

Showing 1 to 4 of 4 rows

Spotting Issues [3/3]

Autonomous Systems

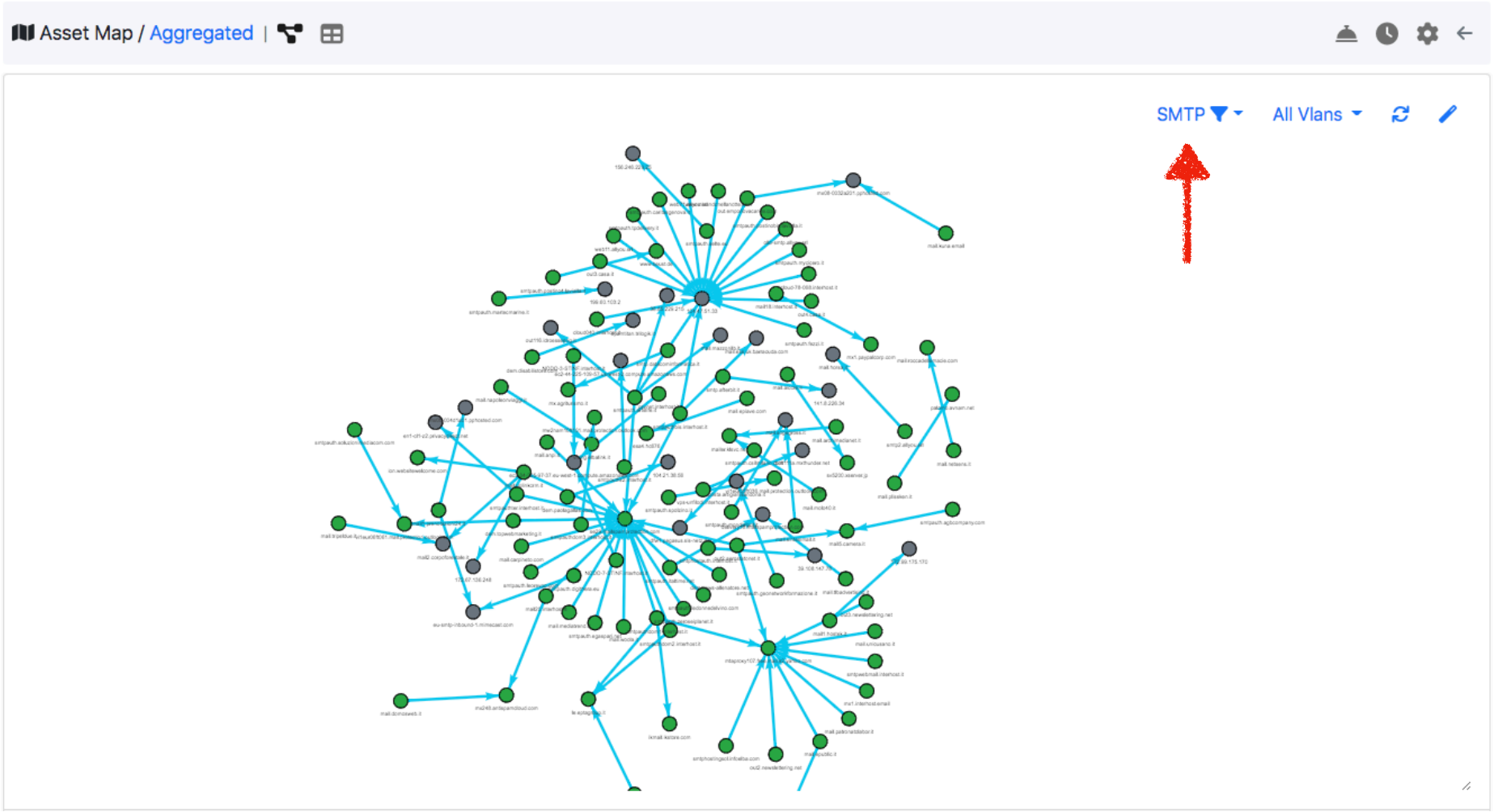
10

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

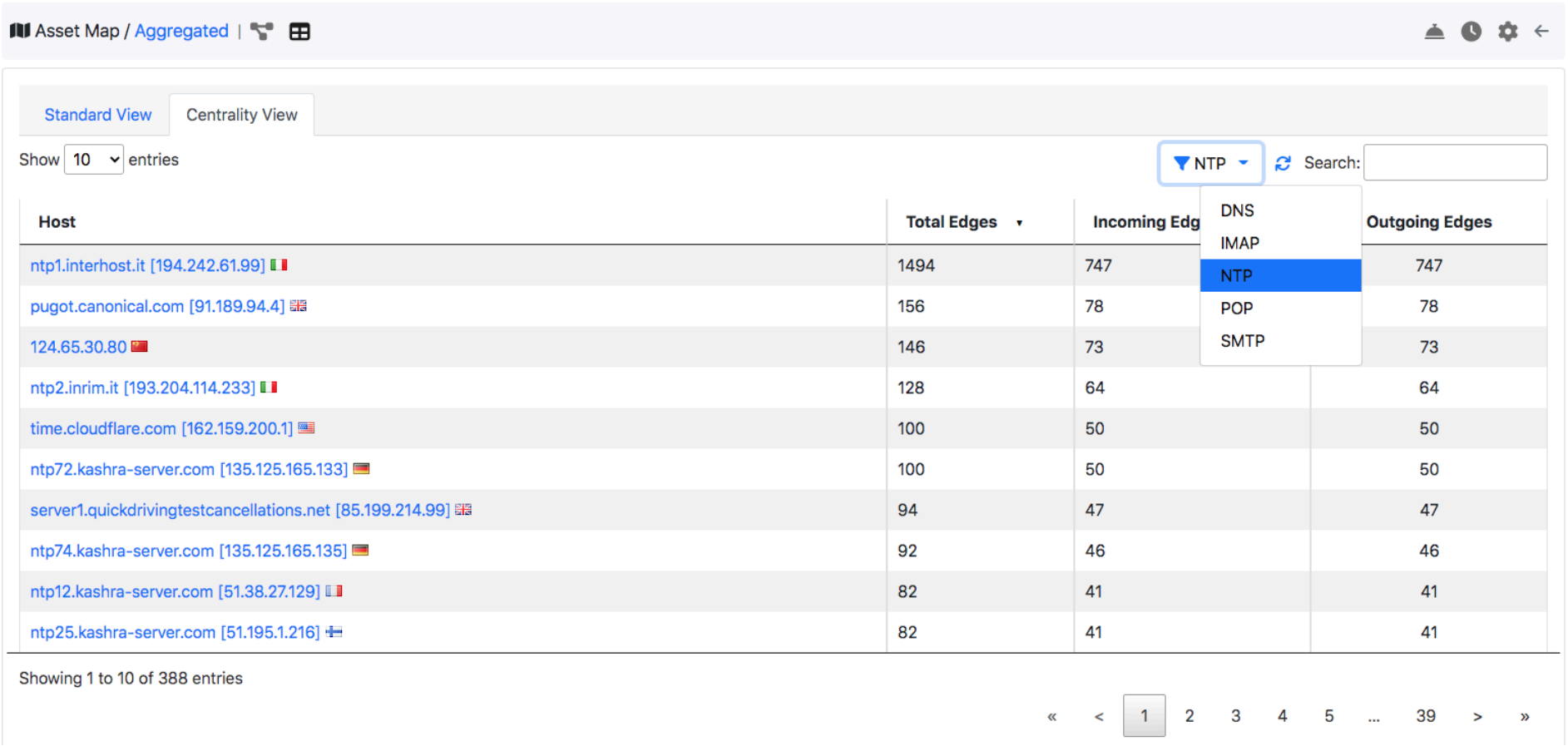
Showing 1 to 10 of 2729 rows

« < 1 2 3 4 5 > »

Know Your Network [1/2]



Know Your Network [2/2]



What about AI ? [1/2]

- Traffic fingerprinting allows network traffic to be clustered according to the sender OS (TCP Fingerprinting) and Application (e.g. JA3/4).

```
194_64_65535_dd5737e4fedb-t13d1516h2_8daaf6152771_9b887d9acb53 [ tiktokv.eu tiktokcdn.com snapchat.com tiktokv.com ]
194_64_65535_dd5737e4fedb-t13d1516ht_8daaf6152771_9b887d9acb53 [ tiktokv.eu ]
2_64_65535_dd5737e4fedb-t13d1516h2_8daaf6152771_e5627efa2ab1 [ googlevideo.com pinimg.com pinterest.com ]
194_64_65535_dd5737e4fedb-t13d1516h2_8daaf6152771_e5627efa2ab1 [ tiktokv.eu tiktokcdn.com snapchat.com tiktokcdn-us.com ]
194_64_65535_dd5737e4fedb-t13d181100_e8a523a41297_d5fe2c511efa [ tiktokcdn.com tiktokv.eu tiktokcdn-eu.com ]
2_64_65535_dd5737e4fedb-t13d1516h2_8daaf6152771_9b887d9acb53 [ tiktokcdn.com ]
2_64_65535_dd5737e4fedb-t12d220700_0d4ca5d4ec72_3304d8368043 [ microsoft.com ryanair.com ]
194_64_65535_dd5737e4fedb-t00d030800_55b375c5d22e_566d5108064c [ facebook.com ]
194_64_65535_dd5737e4fedb-t13d1314h2_f57a46bbacb6_14788d8d241b [ appsflyersdk.com ]
2_64_65535_dd5737e4fedb-t13d2015h2_a09f3c656075_3d00e4afe3b1 [ apple.com ]
2_64_65535_dd5737e4fedb-t00d0310h2_55b375c5d22e_50cc996d9024 [ facebook.com ]
2_64_65535_dd5737e4fedb-t00d030600_55b375c5d22e_8f5d6a331b25 [ facebook.com ]
194_64_65535_dd5737e4fedb-t13d0713gr_04ca88ad2b9b_d8054c94196c [ snapchat.com ]
194_64_65535_dd5737e4fedb-t13d181100_e8a523a41297_ef7df7f74e48 [ tiktokcdn-eu.com ]
194_64_65535_dd5737e4fedb-t13d2015h2_a09f3c656075_3d00e4afe3b1 [ apple.com ]
194_64_65535_dd5737e4fedb-t13d2014ht_a09f3c656075_14788d8d241b [ apple.com icloud.com ]
2_64_65535_dd5737e4fedb-t13d2014ht_a09f3c656075_14788d8d241b [ apple.com spotify.com cdn-apple.com ]
194_64_65535_d3a424420f2a-t13d2015h2_a09f3c656075_3d00e4afe3b1 [ icloud.com apple.com ]
2_64_0_dd5737e4fedb-t13d2014ht_a09f3c656075_14788d8d241b [ apple.com ]
2_64_65535_dd5737e4fedb-t12d220600_0d4ca5d4ec72_3304d8368043 [  ]
2_64_65535_d3a424420f2a-t13d2015h2_a09f3c656075_3d00e4afe3b1 [ apple.com ]
194_64_65535_dd5737e4fedb-t13d0311ap_55b375c5d22e_14aed462abe7 [ apple.com ]
194_64_65535_dd5737e4fedb-t13d181200_e8a523a41297_02c8e53ee398 [ tiktokcdn-eu.com ]
194_64_0_dd5737e4fedb-t13d2014h2_a09f3c656075_14788d8d241b [ icloud.com ]
```

What about AI ? [2/2]

- Ok but what is tiktok.com or esnog.net ?

```
deri@dell 245> ./classify.py
- esnog.net...
deri@dell 246> ./duc
deri@dell 246> duckdb ./domains.duck
v1.1.0 fa5c2fe15f
Enter ".help" for usage hints.
D select * from domains where domain = 'esnog.net';
```

domain varchar	name varchar	model varchar	category varchar	description varchar
esnog.net	esnog.net	mistral	network	esnog.net is a non-profit organization that provides DNS resolution services for Cuba. It operate…

esnog.net is a non-profit organization that provides DNS resolution services for Cuba. It operates as an alternative to the official Cuban DNS servers, offering access to uncensored information and enabling Cubans to bypass internet censorship in their country.

```
deri@super 211> ./url_scraper.py
Scraping esnog.net
 {
    "name": "ESNOG",
    "category": "network",
    "description": "The URL provided is for the website of ESNOG (Grupo de Operadores de Red Españoles), a Spanish ISP association. Give
n the content's focus on networking events, infrastructure, and announcements, it can be classified as a network-related website."
   }
```

- Future looks bright !

Coming Soon

12:00-12:30

Enhancing Suricata with Deep Packet Inspection

Alfredo Cardigliano, Luca Deri, and Matteo Biscosi

This talk explores the integration of an open-source Deep Packet Inspection (DPI) framework with Suricata to enhance its threat detection capabilities. Attendees will learn how DPI can provide deeper network visibility and improve threat detection. Additionally, we will demonstrate how DPI can reduce the amount of traffic Suricata processes by filtering out non-essential flows (e.g., streaming or videoconferencing), thereby enhancing overall performance.

Final Remarks

- Over the past 25+ 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.