

Problem Analysis in ntopng

Matteo Biscosi

Many Security Features...

In ntopng we have many cybersecurity features:

- Alerts
- Asset Map
- Device/Mac Add. Tracking
- Flow Alerts Analyzer
- Historical Flows
- Historical Charts
- Host Map
- Inactive Local Hosts
- Periodicity Map
- Ports Analysis
- Service Map
- Traffic Rules
- Vulnerability Scan
- SNMP
- ...

*Highlighted features are new

...but few are know/used

Of all the cybersecurity features we have, usually users:

- Know very few of them
- Don't know how to use them
- Don't know how to combine them

Problem Analysis

- Let's explore those features one by one, analyze them and understand how can they be used for traffic analysis
- See in real scenarios their effectiveness

Alerts

Alerts Explorer

Alerts are really important because report strange behaviors in the network.

However:

- A lot of alerts are triggered
- Too many informations

The result is



Do not look at them

WRONG

Tune Alerts (1/3)

Let's tune checks in order to use them as better as possible:

- Disable not useful checks for the network
- Tune correct threshold where possible
- Exclude specific alerts in certain cases (Enterprise M License)

(After tuning alerts, even more useful recipients can be used)

Tune Alerts (2/3)



Closed network, except for a couple of hosts, there shouldn't be many flows towards remote hosts

Average active flows 30, maybe a little high

Behavioural Checks All Host Interface Local Networks SNMP Flow System Active Monitoring Syslog						
All (25) Enabled (4) Disabled (21)						
Name	Interface	Category	Severity	Description	Values	Action
Countries Contacts			Notice	Trigger an alert when the number of different countries contacted exceeds the threshold	> 100 Contacts (Minute)	
Flow Flood			Error	Trigger an alert when the new client/server Flows/sec exceeds the threshold	> 60 Flows/sec (Minute)	
Score Threshold Exceeded			Error	Trigger an alert when the score of an host exceeds the threshold	> 1 Score (Minute)	
TCP FIN Scan			Error	Trigger an alert when the number of sent/received FINs/min (with no response) exceeds the threshold	> 10 FINs/min (Minute)	

Showing 1 to 4 of 4 rows

Disable All

	192.168.2.1	3	11	Ubiquiti_06:B3:5A	_gateway	01:00:02	250
	192.168.2.75	1	7	D6:72:EF:7C:9F:CB		58:47	251
	192.168.2.83		2	Dell_19:69:CA		56:57	250
	192.168.2.106	1	10079	Routerbo_0D:E4:9E		59:33	250

Score too low as the average is 250

Tune Alerts (3/3)

Alerts Explorer | All 4 Host 3 Interface SNMP Flow MAC Address System Active Monitoring 1 User

Alerts Last Month 18/08/2023 09:47 → 18/09/2023 09:47 Apply

Filters

New classification:
Require Attention & All

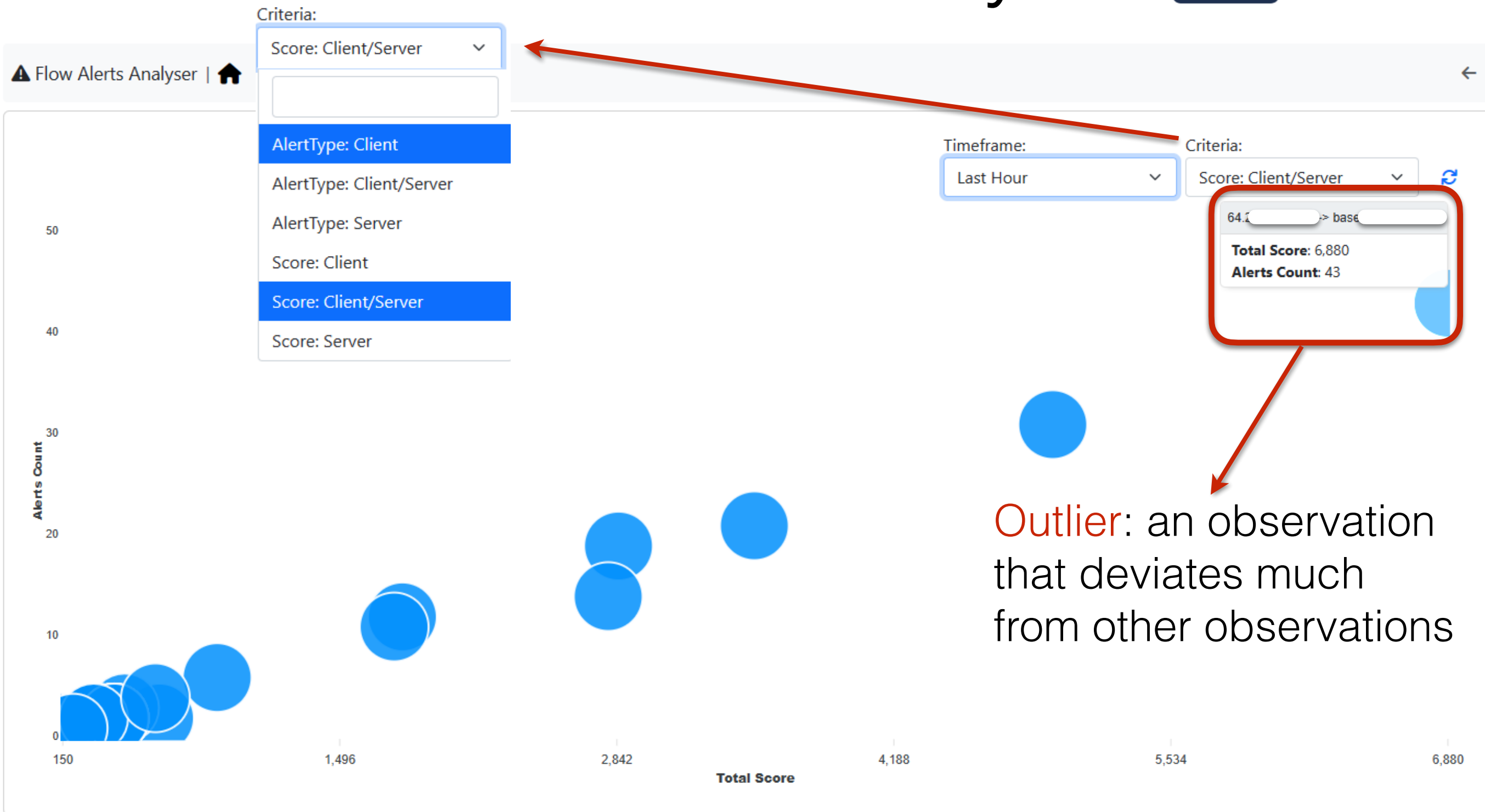
Exclude this alert type towards this host!

Show 10 Entries Top Clients Top Servers Top Alerts Top Applications Top Client Networks Top Server Networks Top DGA Domains

Actions	Date/Time	Score	Category	Application	Alert	Flow	Description
	09/15/2023...	150		TCP:HTTP.UbuntuON...	Binary Application ...	devel:48944 → it.archive.ubuntu.com:80	File Transferred: ...
	09/14/2023...	170		TCP:HTTP DPI	Blacklisted Flow	devel:60382 → 82.85.0.44:8080	Client, server or domain is blacklist
	09/14/2023...	170		TCP:HTTP DPI	Blacklisted Flow	devel:45898 → 82.85.0.44:8080	Client, server or domain is blacklist
	09/14/2023...	170		TCP:HTTP DPI	Blacklisted Flow	devel:42186 → 82.85.0.44:8080	Client, server or domain is blacklist
	09/14/2023...	170		TCP:HTTP DPI	Blacklisted Flow	devel:36988 → 82.85.0.44:8080	Client, server or domain is blacklist
	09/14/2023...	50		UDP:DNS DPI	DNS Data Exfiltration	devel:47369 → _gateway:53	DNS Data Exfiltration
	09/14/2023...	170		TCP:HTTP DPI	Blacklisted Flow	devel:51258 → 82.85.0.44:8080	Client, server or domain is blacklist
	09/13/2023...	150		TCP:HTTP.UbuntuON...	Binary Application ...	devel:44972 → it.archive.ubuntu.com:80	File Transferred: ...
	09/12/2023...	10		TCP:Unknown	Periodic Flow	192.168.2.153:52062 → devel:3001	Periodic Flow ?
	09/12/2023...	20		TCP:HTTP.Google DPI	Periodic Flow	devel:40198 → 142.250.184.78:80	Periodic Flow ?


Are we interested in periodic flows? Otherwise disable the alert

Flow Alerts Analyzer



Host Map

After tuning the Alerts, indicators regarding the score are much more useful

Hosts Map | 



Criteria:

Host Score



"Normal" behavior



Outlier: an observation that deviates much from other observations

Hosts Activity Tracking

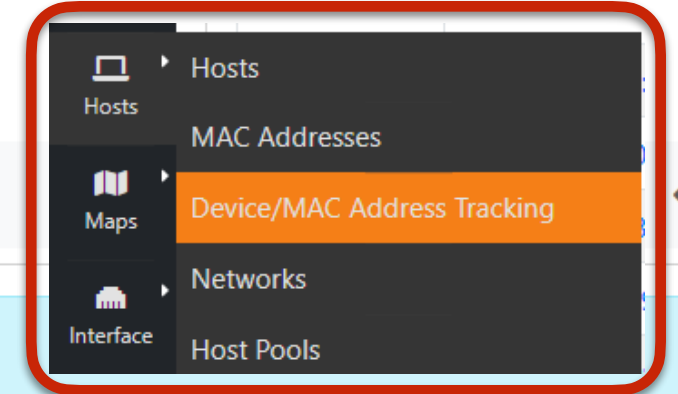
Hosts Tracking

Detect unexpected hosts connecting to the network (with no permission) or trying to attack other local hosts.

It can be detected in a few ways:

- Device/MAC address Tracking (Live)
- Inactive Local Hosts (After the host disconnects)
- SNMP (Live)
- Historical Flows (After)

Device/MAC Address Tracking



Device/MAC Address Tracking List | Devices

What's he doing here?

The Device/MAC Address Tracking is still learning the devices...

Show 10 Entries

+ Search: [] [] [] []

Actions	Device	IP Address	Manufacturer	First Seen	Last Seen	Device Status	Trigger Disconnection Alert
⋮	00:04:96:E4:AA:CD	192.168.2.237	Extreme Networks, Inc.	08:33:02	10:31:53	Denied	×
⋮	AC:1F:6B:AD:6A:2C	192.168.2.134	Super Micro Computer, Inc.	08:33:04	10:31:50	Allowed	×
⋮	00:0C:29:95:B1:4C	fe80::20c:29ff:fe95:b14c	VMware, Inc.	08:32:51	10:33:09	Allowed	×
⋮	0C:C4:7A:CC:4E:6E	fe80::ec4:7aff:fecc:4e6e	Super Micro Computer, Inc.	08:32:34	10:32:34	Allowed	×
⋮	00:0C:29:6C:EB:A2	fe80::20c:29ff:fe6c:eba2	VMware, Inc.	08:33:43	10:32:51	Allowed	×
⋮	20:FD:F1:CB:87:BE	192.168.2.175	3Com Europe Ltd	08:35:01	10:30:15	Allowed	×
⋮	00:0C:29:37:0D:05	fe80::20c:29ff:fe37:d05	VMware, Inc.	08:33:10	10:31:44	Allowed	×
⋮	09:00:09:00:00:67			09:46:15	10:32:15	Allowed	×
⋮	54:9F:35:19:69:C6		Dell Inc.	10:02:29	10:21:29	Allowed	×
⋮	44:A8:42:3B:32:5E	192.168.2.178	Dell Inc.	08:32:00	10:33:05	Allowed	×

When did it happen?

Showing page 1 of 4: total 34 rows

< 1 2 3 4 >





















Do you have a network where hosts do not must disconnect?

Inactive Local Hosts

Hosts | Active **Inactive Local Hosts** 175

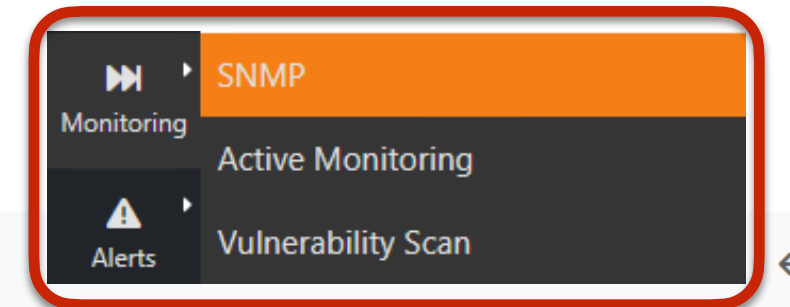
Table View Chart View

Show 10 Entries Device: All Manufacturer: All Network: All VLAN: All

Actions	Host	Name	MAC Address	Manufacturer	First Seen	Last Seen
	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
	192.168.2.129 		00:0C:29:0A:8F:CE	VMware, Inc.	08/04/2023 14:34:08	08/04/2023 14:34:10
	192.168.2.115 		00:0C:29:22:E5:66	VMware, Inc.	08/04/2023 14:34:08	08/04/2023 14:34:10
	192.168.2.39 		00:0C:29:37:0D:05	VMware, Inc.	09/15/2023 15:30:01	09/15/2023 15:30:06
	192.168.2.180 		00:0C:29:41:BD:56	VMware, Inc.	08/04/2023 14:34:08	08/04/2023 14:34:10
	192.168.2.45 		00:0C:29:4C:06:6B	VMware, Inc.	09/01/2023 10:34:30	09/01/2023 10:34:32
	192.168.2.113 		00:0C:29:56:51:96	VMware, Inc.	08/03/2023 14:51:15	08/03/2023 14:51:18
	192.168.2.86@2464 	desktop-8vv8r41	00:0C:29:6C:7D:F6	VMware, Inc.	08/23/2023 17:09:19	08/23/2023 17:12:58
	192.168.2.86@384 [Test vlan] 	desktop-8vv8r41	00:0C:29:6C:7D:F6	VMware, Inc.	08/23/2023 17:09:20	08/23/2023 17:09:25
	192.168.2.86@2223 	desktop-8vv8r41	00:0C:29:6C:7D:F6	VMware, Inc.	08/23/2023 17:09:20	08/23/2023 17:09:25

Showing page 1 of 18: total 175 rows

SNMP



SNMP Devices / MikroTik Ax3 (192.168.2.106) | Interfaces Topology MAC Addresses

Show 10 entries

Search:

Interface Index	MAC Address	IP Associated	Manufacturer	Device Type
2	04:92:26:5C:97:35	fe80::692:26ff:fe5c:9735	ASUSTek COMPUTER INC.	
2	MyDevice (PLC1) [04:18:D6:06:B3:5A]	142.250.184.78 and 4 more Hosts	Ubiquiti Inc	Router/Switch
2	0C:C4:7A:CC:4C:53	fe80::ec4:7aff:fecc:4c53	Super Micro Computer, Inc.	
2	34:DB:FD:80:D9:A6	fe80::36db:fdff:fe80:d9a6	Cisco Systems, Inc	
2	48:A9:8A:0D:E4:9E	192.168.2.106	Routerboard.com	Router/Switch
2	00:E0:2B:00:00:01		Extreme Networks, Inc.	Router/Switch
2	00:0C:29:4C:06:6B	fe80::20c:29ff:fe4c:66b	VMware, Inc.	Computer
2	00:25:90:D4:C8:8C	fe80::225:90ff:fed4:c88c	Super Micro Computer, Inc.	
2	0C:C4:7A:CC:4E:6E	fe80::ec4:7aff:fecc:4e6e	Super Micro Computer, Inc.	
2	3C:4A:92:90:E0:80	192.168.2.169	Hewlett Packard	

Showing 1 to 10 of 21 entries

« < 1 2 3 > »

On which Interface, which host (with IP and MAC) connected

Historical Flows

Historical Flows | **Flows** Analysis

☐ Hourly ☒ Flows

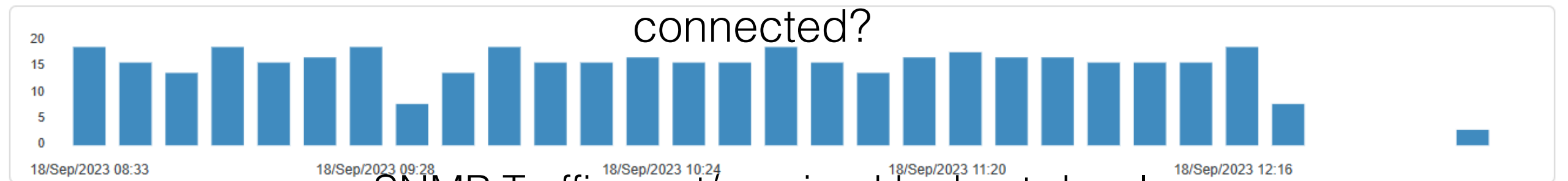
MAC = 00:04:96:E4:AA:CD x Filters

- Edit Host
- Historical Flows
- Delete

00:04:96:E4:AA:CD	192.168.2.75	Extreme Networks, Inc.	08:33:11	13:12:17	Allowed	x
00:04:96:E4:AA:CD	192.168.2.75	Extreme Networks, Inc.	08:32:13	13:12:12	Allowed	x
00:04:96:E4:AA:CD	192.168.2.75	Extreme Networks, Inc.	09:46:15	13:12:20	Allowed	x
00:04:96:E4:AA:CD	192.168.2.237	Extreme Networks, Inc.	08:33:02	13:12:22	Denied	x

Which activity this host did while it was connected?

SNMP Traffic sent/received by host devel



Show 10 Entries

Actions	Begin	End	Duration	Protocol	Application	Score	Flow	Pkts	Bytes	Thpt	L7 Category	Flow Risk	Client
	10:30:01	10:30:01	00:01 sec	UDP	SNMP DPI		devel:41928 ↔ 192.168.2.237:161	2	181 Bytes	1.45 kbps	Network		
	10:30:05	10:30:16	00:11 sec	UDP	SNMP DPI		devel:49477 ↔ 192.168.2.237:161	314	57.26 KB	39.09 kbps	Network		
	10:35:01	10:35:01	00:01 sec	UDP	SNMP DPI		devel:52192 ↔ 192.168.2.237:161	2	181 Bytes	1.45 kbps	Network		
	10:35:05	10:35:15	00:10 sec	UDP	SNMP DPI		devel:41600 ↔ 192.168.2.237:161	308	55.9 KB	41.63 kbps	Network		
	10:40:00	10:40:00	00:01 sec	UDP	SNMP DPI		devel:59314 ↔ 192.168.2.237:161	2	181 Bytes	1.45 kbps	Network		
	10:40:04	10:40:14	00:10 sec	UDP	SNMP DPI		devel:48900 ↔ 192.168.2.237:161	312	56.9 KB	42.38 kbps	Network		
	10:45:00	10:45:00	00:01 sec	UDP	SNMP DPI		devel:38852 ↔ 192.168.2.237:161	2	181 Bytes	1.45 kbps	Network		
	10:45:04	10:45:14	00:10 sec	UDP	SNMP DPI		devel:40082 ↔ 192.168.2.237:161	316	57.54 KB	42.85 kbps	Network		
	10:50:00	10:50:00	00:01 sec	UDP	SNMP DPI		devel:45137 ↔ 192.168.2.237:161	2	181 Bytes	1.45 kbps	Network		
	10:50:04	10:50:14	00:10 sec	UDP	SNMP DPI		devel:45490 ↔ 192.168.2.237:161	310	56.51 KB	42.09 kbps	Network		

Flow Tracking


Flows Tracking

We could start from flows, instead of analyzing hosts activity, identifying and discovering suspicious (malicious) traffic.

There are different ways to do it:

- Service/Periodicity/Assets Map
- Server Ports Analysis (Ports Analysis)

Service Map

 Maps / Aggregated | **Service Map** Service Table Periodicity Map Periodicity Table Asset Map Asset Table



All Networks ▾

All Host Pools ▾

All Protocols ▾



Analysis

Maps

Geo Map

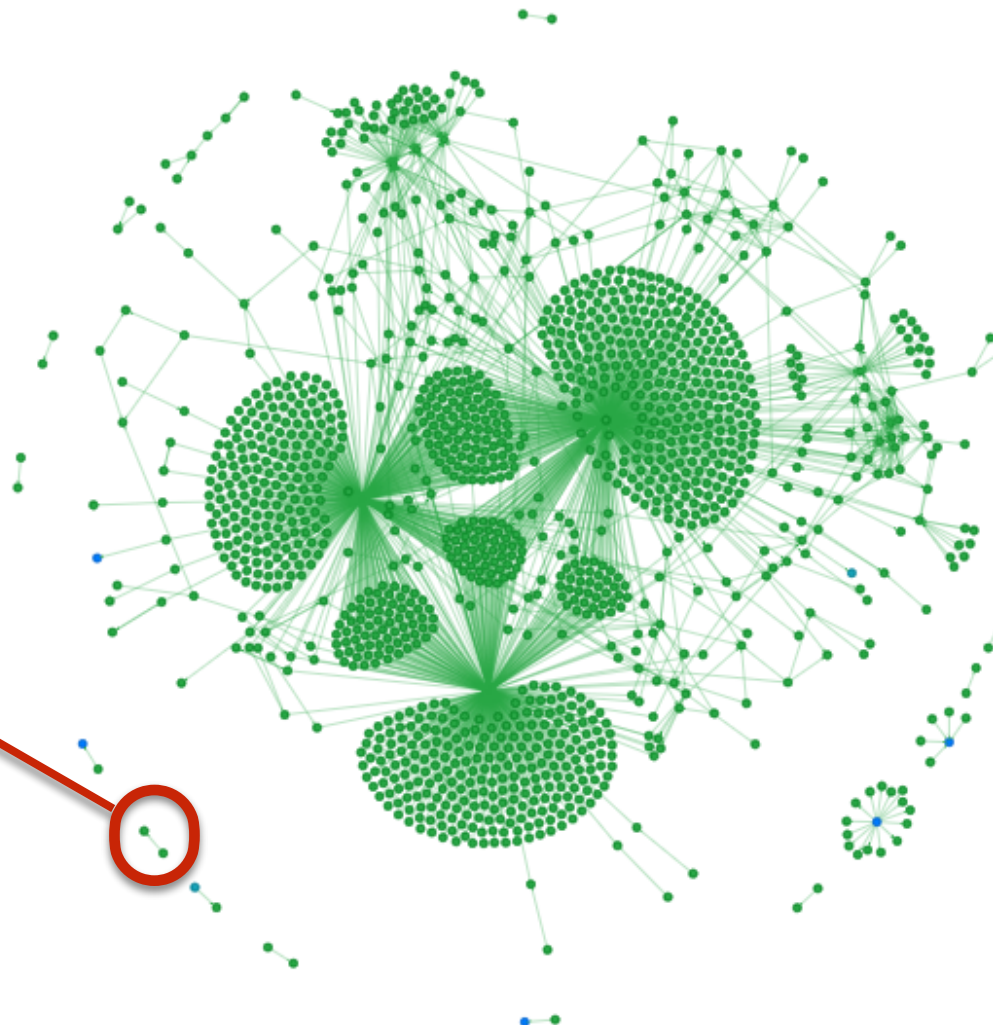


Interface

Hosts

Inside the network
(local traffic), who is
talking to whom?

Is this local traffic legit
or not?




Service Map

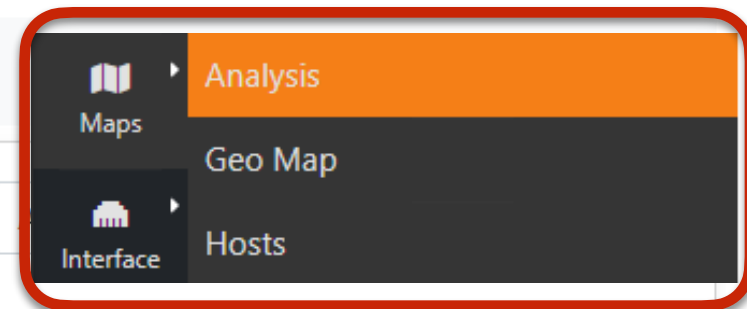
Highly effective against Lateral Movements.

The service map purpose is to show the traffic between local hosts:

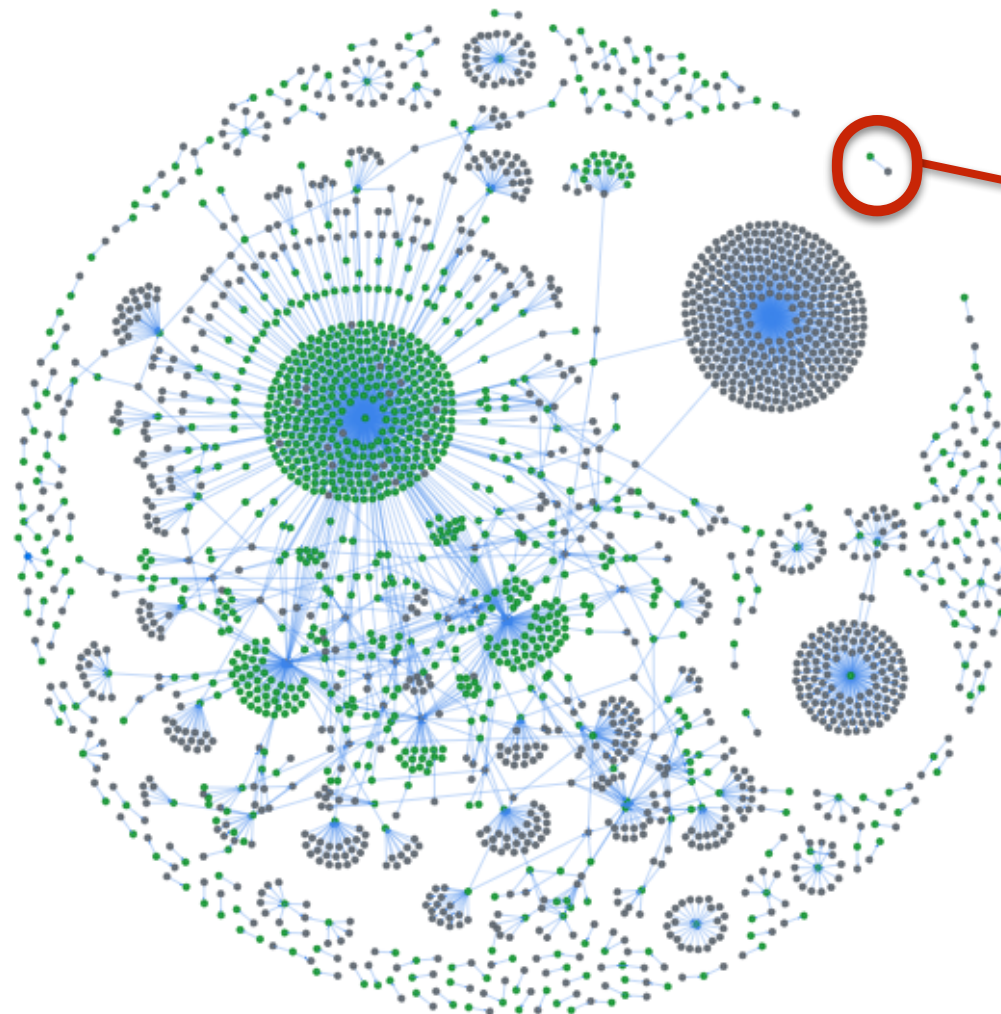
- By using a Learning Period it is possible to let the map learn acceptable local flows and mark the others as denied
- Find possible open ports

Periodicity Map

 Maps / Aggregated | Service Map | Service Table | **Periodicity Map** | Periodicity Table | Asset Map | Asset Table



Which are the periodic flows in a network? is it okay to have them?



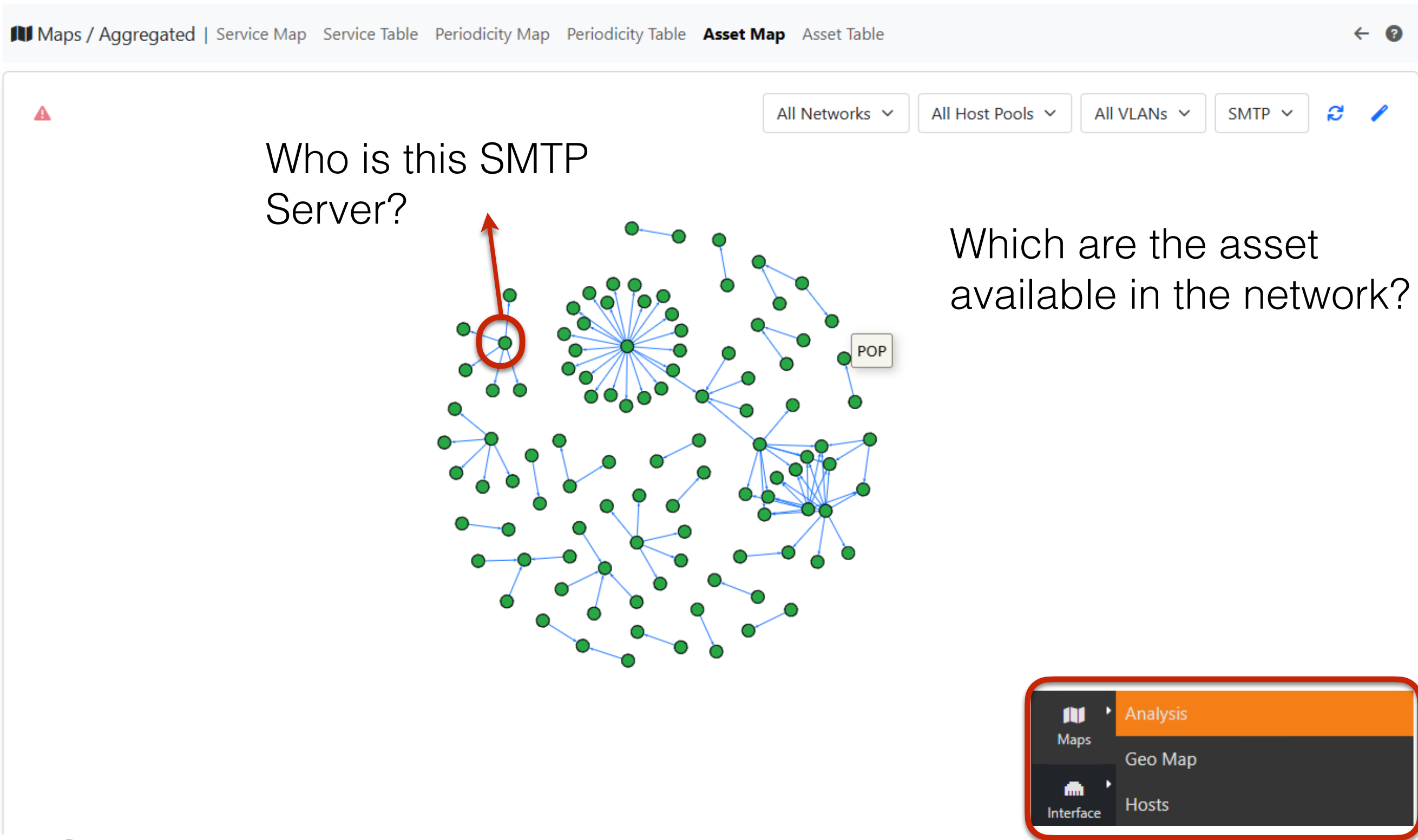
Is this periodic traffic okay?

Periodicity Map

Used to identify Periodic flows:

- Discover the frequency, observations, ...
- Find improper connections (e.g. ssh)

Asset Map

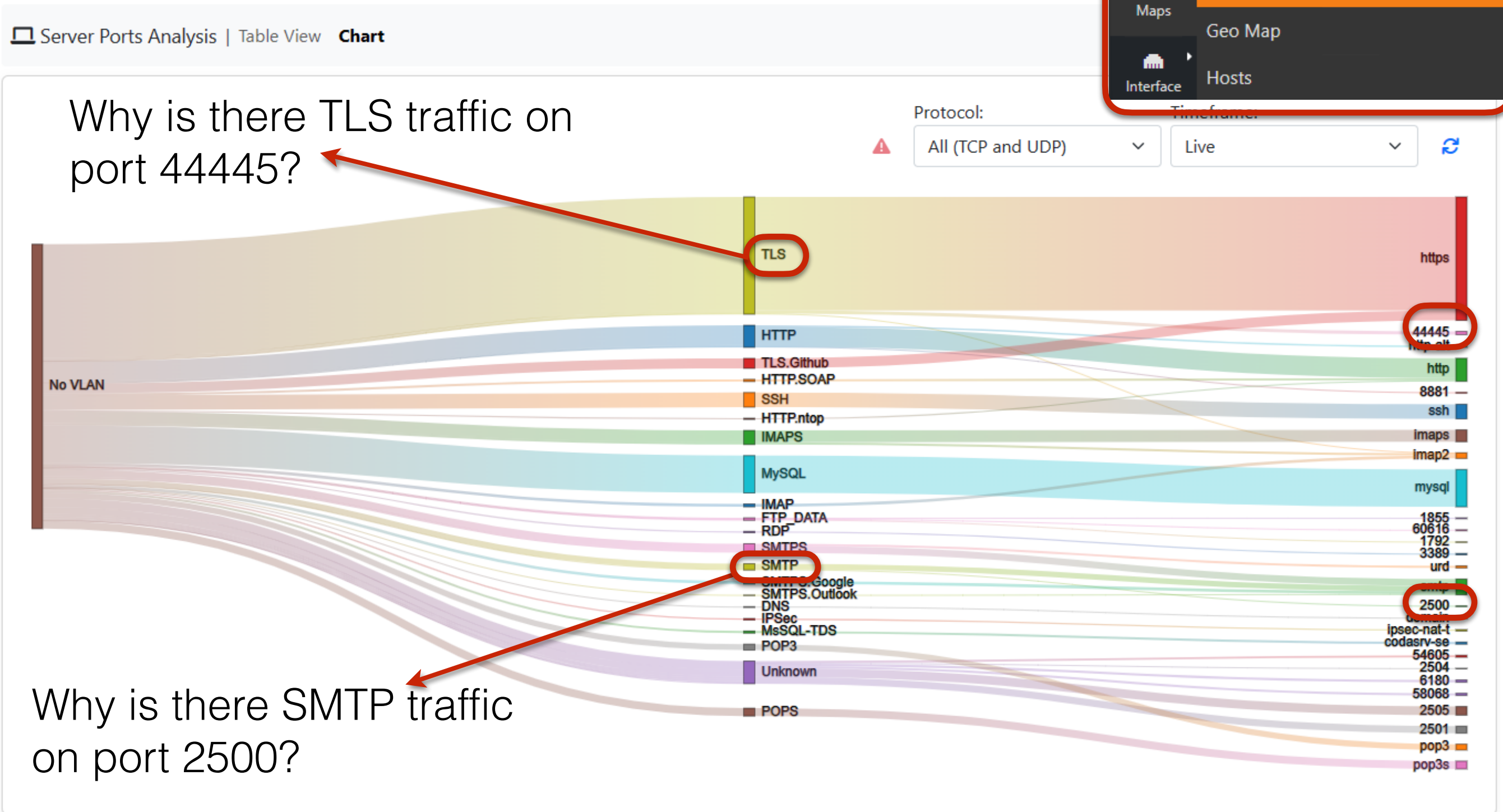


Asset Map

Identify the asset available in a network:

- SMTP, IMAP, POP, DNS, NTP servers
- Identify possible infected hosts, showing themselves as one of those servers

Server Ports Analysis



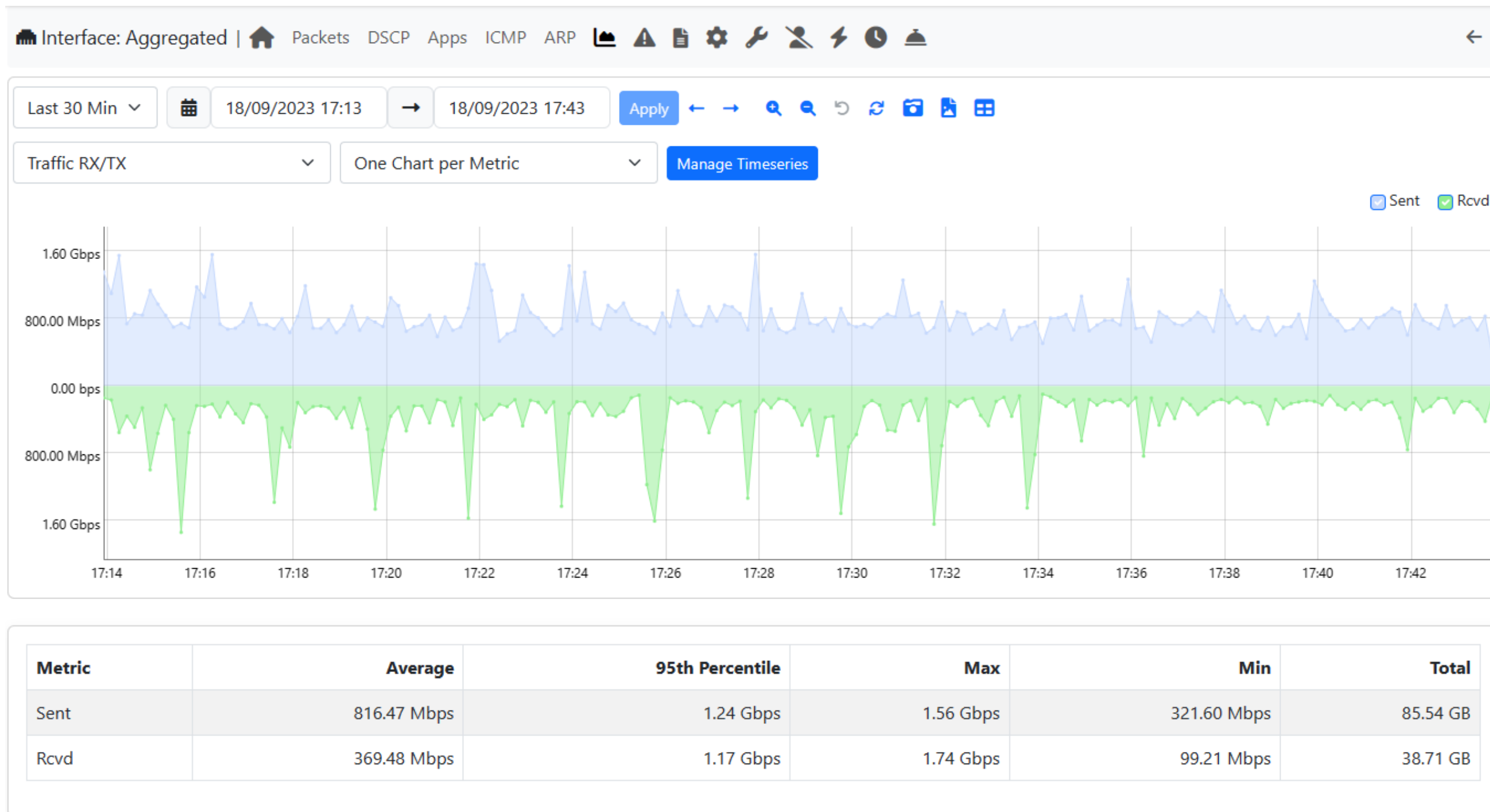
Traffic Rules & Vulnerabilities Scan

- Create custom traffic alerts on Interfaces, Hosts, SNMP Hosts, ...
- Actively scan hosts for their open ports, vulnerabilities, ecc.

We will see more later on with Nicolò...

Historical Charts

Historical Charts

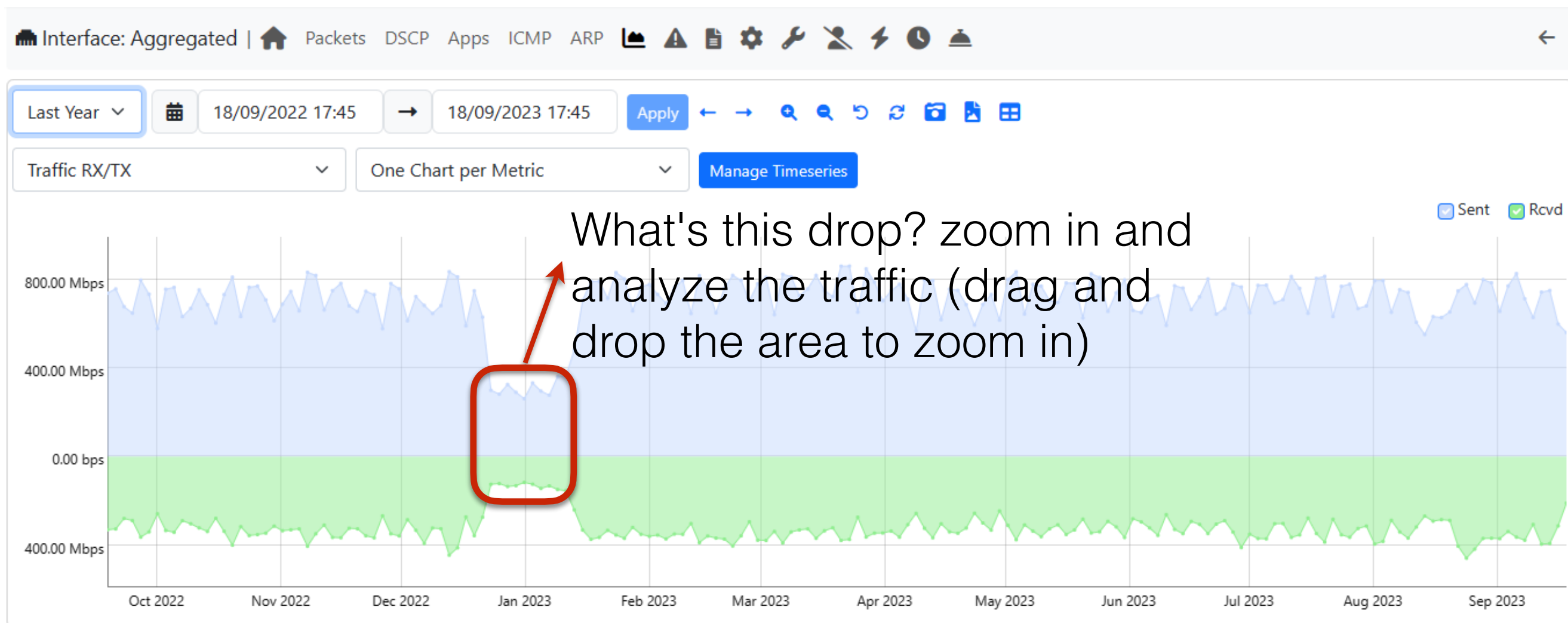


Historical Charts (1/2)

Historical charts page is one of the most important ones for traffic/cybersecurity analysis:

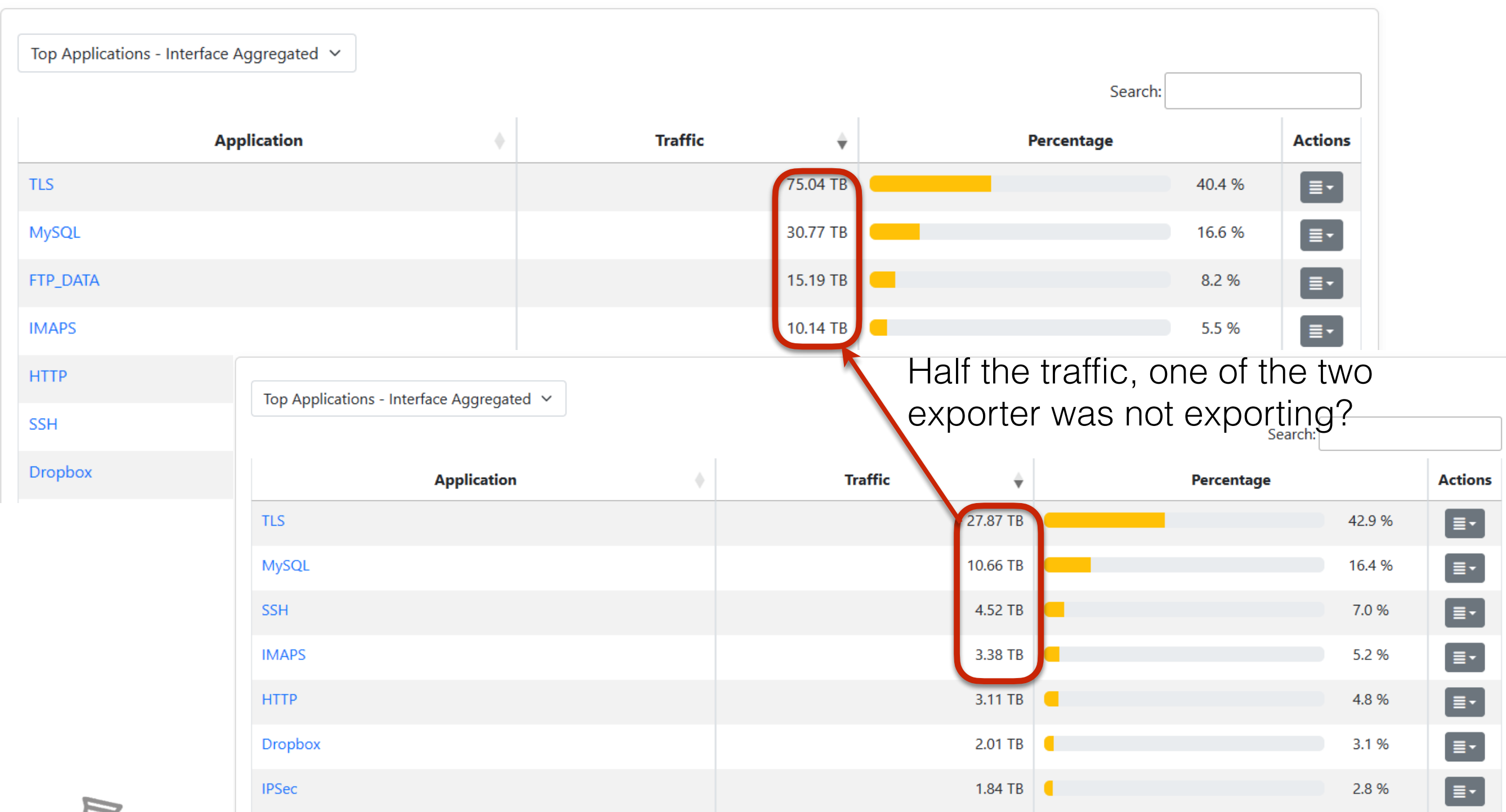
- Useful to identify traffic anomalies
- One of the starting point for traffic analysis

Historical Charts



Metric	Average	95th Percentile	Max	Min	Total
Sent	700.02 Mbps	818.75 Mbps	860.46 Mbps	261.46 Mbps	252.12 TB
Rcvd	325.36 Mbps	395.45 Mbps	459.16 Mbps	116.94 Mbps	117.18 TB

Historical Charts



Try it

Now let's use a couple of pcaps to check how to use all these cybersecurity tools