

ntop 2Q23 Webinar

Highlights

Title	Speaker
Introduction, OT Monitoring, Aggregated Flows, Zoom/Teams Monitoring, OpenAPI	Luca Deri
SNMP Devices/Host Traffic Rules, Server Port Analysis	Nicolò Maio
Live vs Inactive Monitoring, New GUI: Tables and Charts	Matteo Biscosi
Smart Recording, Suricata/Zeek at 100Gbit, New Licensing Model	Alfredo Cardigliano
Open Discussion	



NTOPCONF '23

Call for Paper Deadline JUNE 30TH, 2023

SEPTEMBER 21 (TRAINING)-22 (CONFERENCE), 2023

<https://www.ntop.org/ntopconf2023/>

SCADA/OT Monitoring

Introduction

- ntopng/nProbe have been used in SCADA/OT monitoring for a while.
 - November 2020: Added support IEC 60870-5-104
 - ntopConf 2022: M. Scheu shown how to use ntop tools for monitoring critical infrastructures.
 - Leading OT monitoring companies use ntop tools inside their products.



Network Security Monitoring
in Critical Infrastructure

Martin Scheu
23. June 2022
ntopConf '22

© 2022 Martin Scheu | 1

Ntop and OT/Scada [1/2]

- Ntop tools are not “vertical” tools OT-only but are designed to solving “generic monitoring” problems including:
 - Active/Passive Asset Discovery and Management.
 - Traffic Monitoring.
 - Behavioural Traffic Analysis.
 - Anomaly and vulnerability detection.
 - Threat Intelligence

Ntop and OT/Scada [2/2]

- OT/Scada is supported “à la ntop way” namely”

- Add support in nDPI

44	Modbus	TCP	X	Acceptable	IoT-Scada
244	DNP3	TCP	X	Acceptable	IoT-Scada
245	IEC60870	TCP	X	Acceptable	IoT-Scada
331	TuyaLP	UDP	X	Acceptable	IoT-Scada
332	TPLINK_SHP	TCP/UDP	X	Acceptable	IoT-Scada
334	BACnet	UDP	X	Safe	IoT-Scada

- Implement nProbe Plugin (below ModbusTCP)

```
#
# Timestamp[epoch] SrcIP[ascii:32] DstIP[ascii:32] SrcMAC[ascii:17] DstMAC[ascii:17] SrcPort[uint] DstPort[uint] Protocol[ascii:16]
# TransactionId[uint] ProtocolId[uint] Length[uint] Unit[uint] Function[uint] ReferenceNum[uint] Data[hex:4] Padding[hex:2]
#
1686993895 192.168.3.201 192.168.3.30 18:60:24:97:CE:06 00:D0:C9:EF:D7:C5 54047 502 Modbus/TCP 4313 16 0001 00
1686993895 192.168.3.201 192.168.3.30 18:60:24:97:CE:06 00:D0:C9:EF:D7:C5 54047 502 Modbus/TCP 4314 20 0001 00
1686993895 192.168.3.201 192.168.3.30 18:60:24:97:CE:06 00:D0:C9:EF:D7:C5 54047 502 Modbus/TCP 4315 0001 00
1686993895 192.168.3.201 192.168.3.30 18:60:24:97:CE:06 00:D0:C9:EF:D7:C5 54047 502 Modbus/TCP 4316 18 0001 00
1686993895 192.168.1.201 192.168.1.137 18:60:24:97:CE:06 00:1F:08:02:47:AE 54275 502 Modbus/TCP 556 1039 0010 00
```

- Extend ntopng

ntopng and OT/Scada

- ntopng is able detect, report and alert
 - Unusual error messages
 - Unsupported function calls
 - Function calls that have not been used before
 - Unknown function codes
 - Abnormal protocol behaviour
 - Unexpected state transition
 - Values outside of defined ranges
 - Changes in frequency / periodicity

OT/Scada Behavioural Checks

All (162) Enabled (107) Disabled (55)

Filter Categories Search Script:

Name	Interface	Category	Severity	Description	Values	Action
IEC Invalid Command Transition			Notice	Trigger an alert when a command to/from command or measure to/from command IEC transition is detected		
IEC Invalid Transition			Notice	Trigger an alert when an invalid IEC transition is detected		
IEC Unexpected TypeID			Notice	Trigger an alert when an unexpected TypeID is detected in IEC 104 protocol	9, 13, 36, 45, 46, 48, 30, 103, ...	

All (162) Enabled (107) Disabled (55)

Filter Categories Search Script:

Name	Interface	Category	Severity	Description	Values	Action
ModbusTCP Invalid Transition			Notice	Trigger an alert when an invalid ModbusTCP transition is detected		
ModbusTCP Too Many Exceptions			Error	Trigger an alert when a flow reports a number of exceptions exceeding the specified threshold		
ModbusTCP Unexpected Function Code			Error	Trigger an alert when an unexpected ModbusTCP Function code is detected	3, 6, 16	

Transition/State Monitoring

[ModbusTCP](#)

Function Codes		Registers	
Function	Uses	Register	Uses
Read Holding Registers (3)	1,102	0	1,105
Write Multiple Registers (16)	6	1	1,089
		2	1,089
		7	1,089
		8	1,089
		3	1,089
		5	1,089
		6	1,089
		4	1,089
		9	1,089

Function Code Transitions

Exceptions 16

Behavioural Learning

Traffic Behaviour

Learning Period

Configure the learning period for behavioural traffic analysis.

Hours

Days

2

Service Status During Learning

The default status of a new discovered service when the Service Map is learning.

Undecided

Allowed

Denied

Service Status Post Learning

The default status of a new discovered service when the Service Map has finished the learning.

Undecided

Allowed

Denied

IEC60870 Learning Period

Configure the learning period for IEC60870 and ModbusTCP traffic analysis. Default: 6 hours.

Hours

Days

6

ModbusTCP Learning Period

Configure the learning period for ModbusTCP traffic analysis. Default: 6 hours.

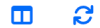
Hours

Days

1

Alerts

Show 10 Entries



Action	Date/Time	Score	Application	Alert	Flow	Description
⋮	12:04:21	100	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:3343 ↔ 172.16.203.5:502	Function Code 'Write Single Regi...
⋮	12:04:21	200	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:3343 ↔ 172.16.203.5:502	1 Exceptions
⋮	12:04:21	300	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:3343 ↔ 172.16.203.5:502	Function Code 'Write Multiple Re...
⋮	12:04:21	100	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:1788 ↔ 172.16.203.5:502	1 Exceptions
⋮	12:04:21	100	TCP:Modbus DPI	ModbusTCP Too Many Exceptions	172.16.203.200:2634 ↔ 172.16.203.5:502	1 Exceptions
⋮	12:04:21	200	TCP:Modbus DPI	ModbusTCP Invalid Function Code	172.16.203.200:2634 ↔ 172.16.203.5:502	Function Code 'Write Multiple Re...
⋮	12:04:21	100	TCP:Modbus DPI	ModbusTCP Invalid Function Code	192.168.3.201:54047 ↔ 192.168.3.30:502	Function Code 'Read Coils (1)' de...

⚠ Alert: ModbusTCP Invalid Function Code | 172.16.203.200:3343 ↔ 172.16.203.5:502 | [Overview](#)

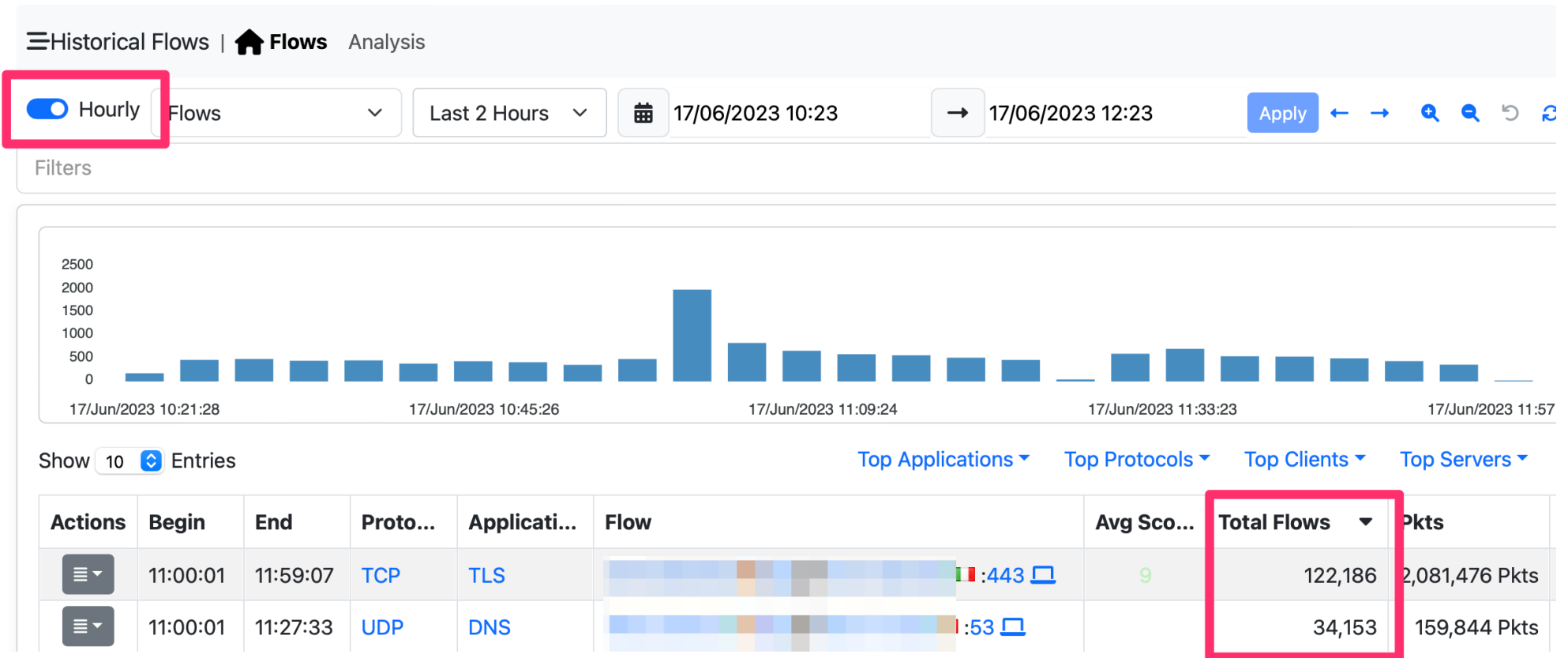
Alert	🔔 ModbusTCP Invalid Function Code						
Flow Peers [Client / Server]	172.16.203.200:3343 ↔ 172.16.203.5:502						
Protocol / Application	TCP:Modbus						
Date/Time	12:05:46						
Score	200						
Description	Function Code 'Write Single Register (6)' detected						
Other Issues	ModbusTCP Too Many Exceptions						
Traffic Info	<table border="1"> <tr> <td>Client to Server Traffic</td> <td>82.15 KB</td> </tr> <tr> <td>Main Direction</td> <td>Server → Client</td> </tr> <tr> <td>Server to Client Traffic</td> <td>139.95 KB</td> </tr> </table>	Client to Server Traffic	82.15 KB	Main Direction	Server → Client	Server to Client Traffic	139.95 KB
Client to Server Traffic	82.15 KB						
Main Direction	Server → Client						
Server to Client Traffic	139.95 KB						

Aggregated Flows

ClickHouse Historical Flows

- ntopng has the ability to:
 - Dump historical flows into ClickHouse.
 - Correlate flows with alerts.
 - Download (n2disk is required) flows with traffic traces.
- Historical flows can be heavy (hundred of million/day) and exhaust disk space.
- What if we can aggregate flows, save disk space, and still have the ability to have accurate “Top X” and alert correlation?

Aggregated Flows [1/2]



Aggregated Flows [2/2]

- Typical savings ratio: 133M vs 648K (1:200)



Processed 12,934,942 records [133,967,482 records/sec].



Processed 13,750 records [648,893 records/sec].

- Flexible Settings

ClickHouse

ClickHouse Aggregated Flows Data Retention
Number of days to keep aggregated flows informations (it must be larger than unaggregated flows retention). Default: 60 days.

ClickHouse Limit Aggregated Flows
Number of maximum aggregated flow entries to insert every hourly dump.

ClickHouse Minimum Aggregated Flow Traffic
Discard aggregated flows whose size is less that the specified value (in KBytes).

Include Alerted Flows
Include all alerted flows in aggregated flows.

[Save](#)

- Next Step: Aggregate Alerts

Zoom and MS Teams Monitoring

Zoom/MS Teams Monitoring [1/2]

- nDPI has been enhanced...

38	Skype_TeamsCall	TCP	Acceptable	VoIP
125	Skype_Teams	UDP	Acceptable	VoIP
189	Zoom	TCP	Acceptable	Video
250	Teams	TCP	Safe	Collaborative

- nProbe has been Enhanced to handle STUN/RTP flows with “non-standard”

[NFv9 57626] [IPFIX 35632.154] [Len 4]	%RTP_IN_JITTER	RTP jitter (ms * 1000)
[NFv9 57627] [IPFIX 35632.155] [Len 4]	%RTP_OUT_JITTER	RTP jitter (ms * 1000)
[NFv9 57628] [IPFIX 35632.156] [Len 4]	%RTP_IN_PKT_LOST	Packet lost in stream (src->dst)
[NFv9 57629] [IPFIX 35632.157] [Len 4]	%RTP_OUT_PKT_LOST	Packet lost in stream (dst->src)
[NFv9 57902] [IPFIX 35632.430] [Len 4]	%RTP_IN_PKT_DROP	Packet discarded by Jitter Buffer (src->dst)
[NFv9 57903] [IPFIX 35632.431] [Len 4]	%RTP_OUT_PKT_DROP	Packet discarded by Jitter Buffer (dst->src)
[NFv9 57633] [IPFIX 35632.161] [Len 1]	%RTP_IN_PAYLOAD_TYPE	RTP payload type
[NFv9 57630] [IPFIX 35632.158] [Len 1]	%RTP_OUT_PAYLOAD_TYPE	RTP payload type
[NFv9 57631] [IPFIX 35632.159] [Len 4]	%RTP_IN_MAX_DELTA	Max delta (ms*100) between consecutive pkts (src->dst)
[NFv9 57632] [IPFIX 35632.160] [Len 4]	%RTP_OUT_MAX_DELTA	Max delta (ms*100) between consecutive pkts (dst->src)
[NFv9 57820] [IPFIX 35632.348] [Len 64	varlen] %RTP_SIP_CALL_ID	SIP call-id corresponding to this RTP stream
[NFv9 57906] [IPFIX 35632.434] [Len 4]	%RTP_MOS	RTP pseudo-MOS (value * 100) (average both directions)
[NFv9 57842] [IPFIX 35632.370] [Len 4]	%RTP_IN_MOS	RTP pseudo-MOS (value * 100) (src->dst)
[NFv9 57904] [IPFIX 35632.432] [Len 4]	%RTP_OUT_MOS	RTP pseudo-MOS (value * 100) (dst->src)
[NFv9 57908] [IPFIX 35632.436] [Len 4]	%RTP_R_FACTOR	RTP pseudo-R_FACTOR (value * 100) (average both directions)
[NFv9 57843] [IPFIX 35632.371] [Len 4]	%RTP_IN_R_FACTOR	RTP pseudo-R_FACTOR (value * 100) (src->dst)
[NFv9 57905] [IPFIX 35632.433] [Len 4]	%RTP_OUT_R_FACTOR	RTP pseudo-R_FACTOR (value * 100) (dst->src)
[NFv9 57853] [IPFIX 35632.381] [Len 4]	%RTP_IN_TRANSIT	RTP Transit (value * 100) (src->dst)
[NFv9 57854] [IPFIX 35632.382] [Len 4]	%RTP_OUT_TRANSIT	RTP Transit (value * 100) (dst->src)
[NFv9 57852] [IPFIX 35632.380] [Len 4]	%RTP_RTT	RTP Round Trip Time (ms)

Zoom/MS Teams Monitoring [2/2]

- And ntopng too...

Skype_TeamsCall Flows 0 bps | Total Bytes: 1.22 MB
0 bps | Total Throughput: 0 bps Flow Idle Timeout: 60 sec

10 Hosts Status Severity Direction L7 Protocol Categories DSCP Host Pool Networks IP Version Protocol

Serial	Application	Proto	Client	Server	Duration	Score	Breakdown	Actual Thpt	Total Bytes	Info
	STUN.Skype_T... DPI	UDP !	imacm1 R :50014	host-82-51-138-80.retail.telecomital... R :59225	< 1 sec	50	Client Server	0 bps	726.86 KB	Audio Stream
	STUN.Skype_T... DPI	UDP !	192.168.1.125 R :50042	imacm1 R :50044	< 1 sec	50	Server	0 bps	400.04 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP i	imacm1 R :50054	52.114.227.13 R :nat-stun-port	< 1 sec	10	Client	0 bps	58.76 KB	Audio Stream
	STUN.Skype_T... DPI	UDP	imacm1 R :50014	52.114.227.31 R :nat-stun-port	< 1 sec		Client	0 bps	8.87 KB	Audio Stream
	STUN.Skype_T... DPI	UDP i	imacm1 R :50020	52.114.227.44 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.74 KB	Audio Stream
	STUN.Skype_T... DPI	UDP i	imacm1 R :50032	52.114.227.38 R :nat-stun-port	< 1 sec	10	Client	0 bps	7.31 KB	Audio Stream
	STUN.Skype_T... DPI	UDP !	imacm1 R :50032	host-82-51-138-80.retail.telecomital... R :57022	< 1 sec	50	Client	0 bps	7.03 KB	Video Stream
	STUN.Skype_T... DPI	UDP !	imacm1 R :50054	host-82-51-138-80.retail.telecomital... R :52292	< 1 sec	50	Client	0 bps	5.46 KB	Screen Sharing Stream
	STUN.Skype_T... DPI	UDP i	imacm1 R :50044	52.114.227.31 R :nat-stun-port	< 1 sec	10	Client	0 bps	3.4 KB	Audio Stream
	STUN.Skype_T... DPI	UDP !	imacm1 R :50020	host-82-51-138-80.retail.telecomital... R :49621	< 1 sec	50	Client	0 bps	3.27 KB	Video Stream

Flow: 192.168.1.29:50014 ↔ 82.51.138.80:59225 | Overview

Flow Peers [Client / Server]	imacm1 R P :50014 [9C:58:3C:A7:EE:CC] ↔ host-82-51-138-80.retail.telecomitalia.it R :59225 [10:13:31:F1:39:76]
Protocol / Application	UDP / STUN.Skype_TeamsCall (VoIP) [Confidence: DPI] [! Audio Stream]

Finally... OpenAPI

The screenshot shows the ntopng REST API documentation interface. On the left is a dark sidebar with navigation icons and labels: ntopng logo, Shortcuts, Dashboard, Alerts, Flows, Hosts, Flow Exp., Maps, Interface, Settings, and Developer. The main content area has a top navigation bar with 'Aggregated' (with a refresh icon), a search bar, and notification/user icons. Below this, the page title is 'ntopng 5.7' with a version badge, followed by the API path '/misc/rest-api-v2.json' and the subtitle 'ntopng RESTful API documentation'. A 'Schemes' dropdown menu is set to 'HTTPS'. The 'Interfaces' section is titled 'Everything about interfaces' and contains a table of API endpoints. The first endpoint is a GET request to '/lua/rest/v2/get/interface/data.lua' with the description 'Get interface data'. Below the endpoint name, it states 'Interface data is returned'. A 'Parameters' section is visible at the bottom of the endpoint card, and a 'Try it out' button is located to the right of the parameters section. The 'REST API' category in the sidebar is highlighted in orange.

Presentation Outline

- SNMP Devices Rules
- Host/Network Interface Rules
- Server Ports Analysis Page

PS: All the features displayed on this presentation are available only from Enterprise L license or superior.

Nicolo' Maio
maio@ntop.org

SNMP Devices Rules [1/3]

- Monitoring several SNMP devices in order to unveil changes and changed trends in traffic, can be difficult.
- SNMP Devices Rules enables the creation of periodic checks (for all or a selected SNMP device) at a specific frequency (5 mins, 1 hour, or 1 day).
- The triggered rules will emit a “Threshold Crossed” alert when a SNMP Device exceeds (up or down) the specified threshold (Packets, Bytes or Interface Errors).
- Available only from Enterprise L license or superior.

SNMP Devices Rules [2/3]

Select the SNMP device

Select the SNMP device port

Select the metric

Select the check frequency

Select the rule threshold

Add Rule

Rule type SNMP Device

Device 3Com Baseline Switch (192.168.2.175)

Interface GigabitEthernet1/0/10 (10)

Metric Bytes (RX/TX)

Check Frequency 5 Minutes

Threshold Volume < KB MB GB > < > 1

NOTES

- Device: select the SNMP Device to be analyzed
- Interface: select the interface of the SNMP device that needs to be analyzed.
- Metric: select the metric to be analyzed (e.g. errors -> the SNMP metric errors)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculated between the last two frequency checks (e.g. <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)

SNMP Devices Rules [3/3]

ens160 199.90 Mbps 213.30 Kbps 2 17 3 12 575 Search

Alerts Explorer | All 2 Host 2 Interface **SNMP** Flow MAC Address System User

Past Ack Engaged Last 30 Min 15/06/2023 09:04 → 15/06/2023 09:34 Apply

Severity **Error** Filters

Show 10 Entries Search:

	Device IP	SNMP Interface	SNMP Device Name	Counts	Description
Id Crossed	192.168.2.237	X435-24P-4S Port 2	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 7	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 15	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 14	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 15	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB
Id Crossed	192.168.2.237	X435-24P-4S Port 7	X435-24P-4S	1	Metric: Bytes (RX/TX) / Unit: Volume / Value: 0 Bytes / Threshold: < 1 GB

Host/Interface Rules [1/3]

- Same as SNMP Rules but for hosts and interfaces.
- Frequency of 5 mins, 1 hour or 1 day.
- The triggered rules will emit a “Threshold Crossed” alert when a Host or a Network Interface exceeds (up or down) the specified threshold (Traffic, Score or Specific Application Traffic).
- Available only from Enterprise L license or superior.

Host/Interface Rules [2/3]

In case of Rule Type Host
indicate the Host,
Otherwise select an Interface

Select the metric

Select
the check frequency

Select the rule threshold

Add Rule

Rule type Host Interface

Target

Metric

Check Frequency

Threshold KB MB GB > <

NOTES

- Target: insert the IP of a Local Host to be analyzed or a * (meaning that all Local Hosts has to be analyzed) or select a local network interface
- Metric: select the metric to be analyzed (e.g. DNS -> the DNS traffic)
- Frequency: select the frequency of the analysis (e.g. 5 Min -> analyzed every 5 minutes)
- Threshold: select the type of threshold (Volume, Throughput or Percentage), lowerbound or upperbound, and the threshold that, if exceeded, is going to trigger an alert
- Percentage Threshold: is calculated beetwen the last two frequency checks (e.g. <1% with frequency 5 Min -> if the difference between precedent frequency and the last 5 minutes check is lower than 1% trigger and alert)

Add

Host/Interface Rules [3/3]

The screenshot shows the ntopng interface for the 'Hosts' section. At the top, there's a status bar for 'ens160' showing network activity (32.70 Mbps, 931.80 Kbps) and various system metrics (3 alerts, 20 CPU, 12 RAM, 15 disk, 956 network). A search bar is also present. The main content area is titled 'Local Traffic Rules' and displays a table with 2 entries. The first entry is for 'ens160' with a type of 'Interface', metric of 'Traffic', check frequency of '5 Minutes', and a threshold of '> 15 %'. The second entry is for '*' with a type of 'Host', metric of 'Traffic', check frequency of '5 Minutes', and a threshold of '< 1 GB'. The 'Actions' column for the 'ens160' rule is highlighted with a red box. A red arrow points from the text 'In Actions menu the edit and delete rule options are present' to this box. Below the table, it says 'Showing 1 to 2 of 2 entries' and a pagination control shows '1'. A 'NOTES' section contains instructions on how to trigger alerts, add new rules, and remove rules. The footer includes version information (ntopng Enterprise XL v.5.7.230503), copyright (© 1998-23 - ntop), and system time (15:11:38 +0000 UTC | Uptime: 24:06).

Target	Type	Metric	Check Frequency	Threshold	Actions
ens160	Interface	Traffic	5 Minutes	> 15 %	[Actions]
*	Host	Traffic	5 Minutes	< 1 GB	[Actions]

In Actions menu the edit and delete rule options are present

Server Ports Analysis [1/2]

- Monitoring available host services is not simple with live traffic view. On the other hand it is important to keep an eye on new or disappeared server port (service map).
- In order to enable it, start selecting a Network Protocol, then an Application Protocol and the server port.
- The page displays many server local host details including:
 - Host IP
 - Host Name
 - MAC address
 - Manufacturer
 - Host Total Score
 - Host Total Flows
 - Host Total Traffic.
- Available only from Enterprise L license or superior.

Server Ports Analysis [2/2]

Select the Protocol

Select the Application

Select the Server port

The screenshot shows the ntop Server Ports Analysis interface. At the top, there are three dropdown menus: 'Protocol: UDP', 'Application: DNS', and 'Server Port: 53 (1)'. Red arrows point from the text labels above to these dropdowns. Below the filters, there is a table with the following data:

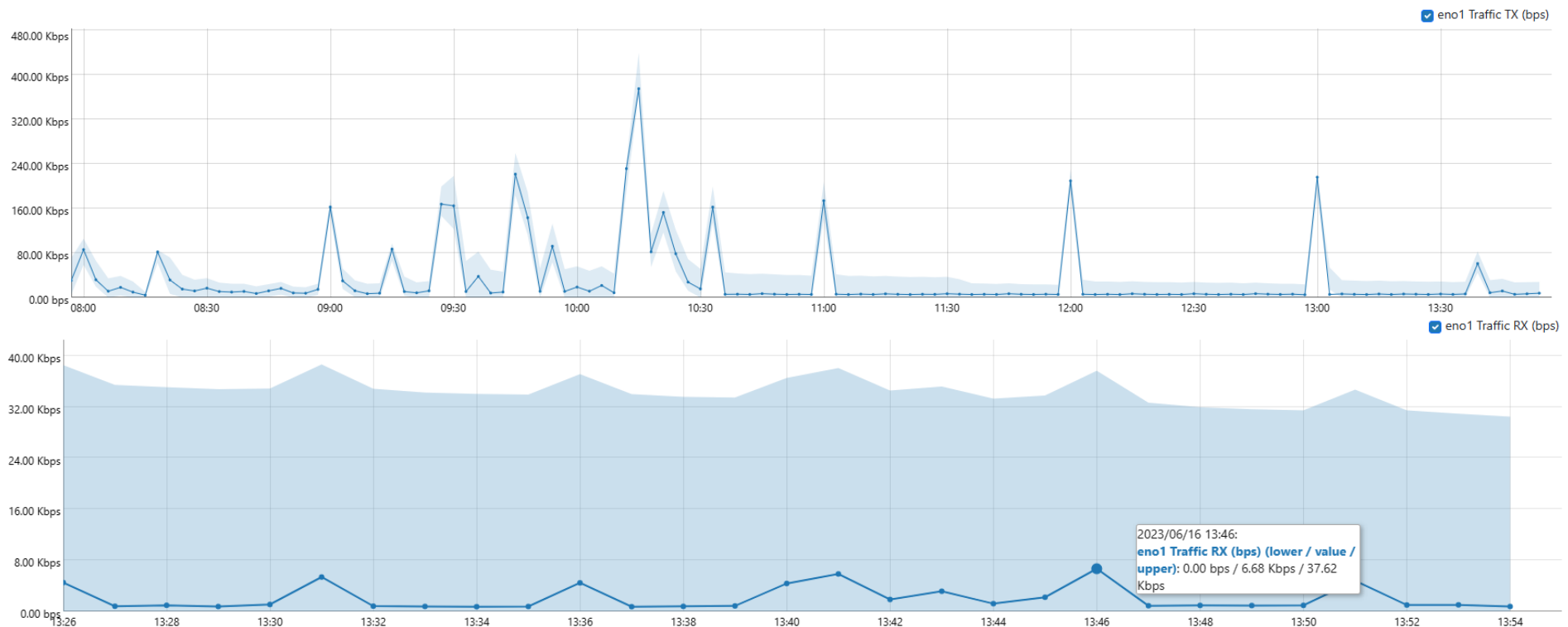
IP	Host Name	MAC	Manufacturer	Total Score
192.168.2.1	_gateway	04:18:D6:06:B3:5A	Ubiquiti Inc	

Below the table, it says 'Showing page 1 of 1: total 1 rows'. The footer of the interface includes 'ntopng Enterprise XL v.5.7.230503 (Ubuntu 22.04.1 LTS)', '© 1998-23 - ntop', and '09:54:33 +0000 UTC | Uptime: 04:50'. A sidebar on the left contains navigation icons for Shortcuts, Dashboard, Alerts, Flows, Hosts, Maps, Interface, Settings, Developer, and Help.

Behavior Analysis & Inactive Hosts

Behavior Analysis (1/2)

- Use algorithms to understand and foresee the behaviors of hosts and interfaces
- See the actual value and the lower/upper bound of the foreseen value



Behavior Analysis (2/2)

The value exceeds the lower or upper bound













Trigger the corresponding alert

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

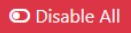
All (15) Enabled (11) Disabled (4)

Filter Categories Search Script: behavior

Name	Interface	Category	Severity	Description	Values	Action
Unexpected Score Behaviour			Error 	Trigger an alert when an unexpected score is identified.		 
Unexpected Traffic Behaviour			Error 	Trigger an alert when an unexpected amount of traffic is identified.		 

Showing 1 to 2 of 2 rows

« < 1 > »



Inactive Hosts Analysis (1/2)

- Which Host is active and which is inactive?
- When was active the last time on the net?
- Which MAC address did it have?
- First time in ntopng that inactive data are shown (usually only live data are present)

Inactive Hosts Analysis (2/2)

Hosts | Active Inactive ⁷

Local Hosts

Show 10 Entries

Actions	IP Address	VLAN	MAC Address	Name	First Seen	Last Seen
	fe80::20c:29ff:fe22:e566		00:0C:29:22:E5:66	VMware, Inc.	13:03:06	13:03:07
	192.168.2.126		00:0C:29:22:E5:66	VMware, Inc.	08:00:15	08:00:16
	fe80::225:90ff:fed4:ccf9		devel	Super Micro Computer, Inc.	13:15:56	13:15:58
	192.168.2.209		94:E9:79:E4:07:7B	Liteon Technology Corporation	08:00:16	08:00:17
	192.168.2.208		E4:5E:37:AF:C9:E0	Intel Corporate	08:00:16	08:00:17
	192.168.2.167		34:DB:FD:80:D9:A6	Cisco Systems, Inc	13:15:00	13:15:01
	192.168.2.198		98:01:A7:A5:0C:93	Apple, Inc.	08:00:16	08:00:17

Showing page 1 of 1: total 7 rows

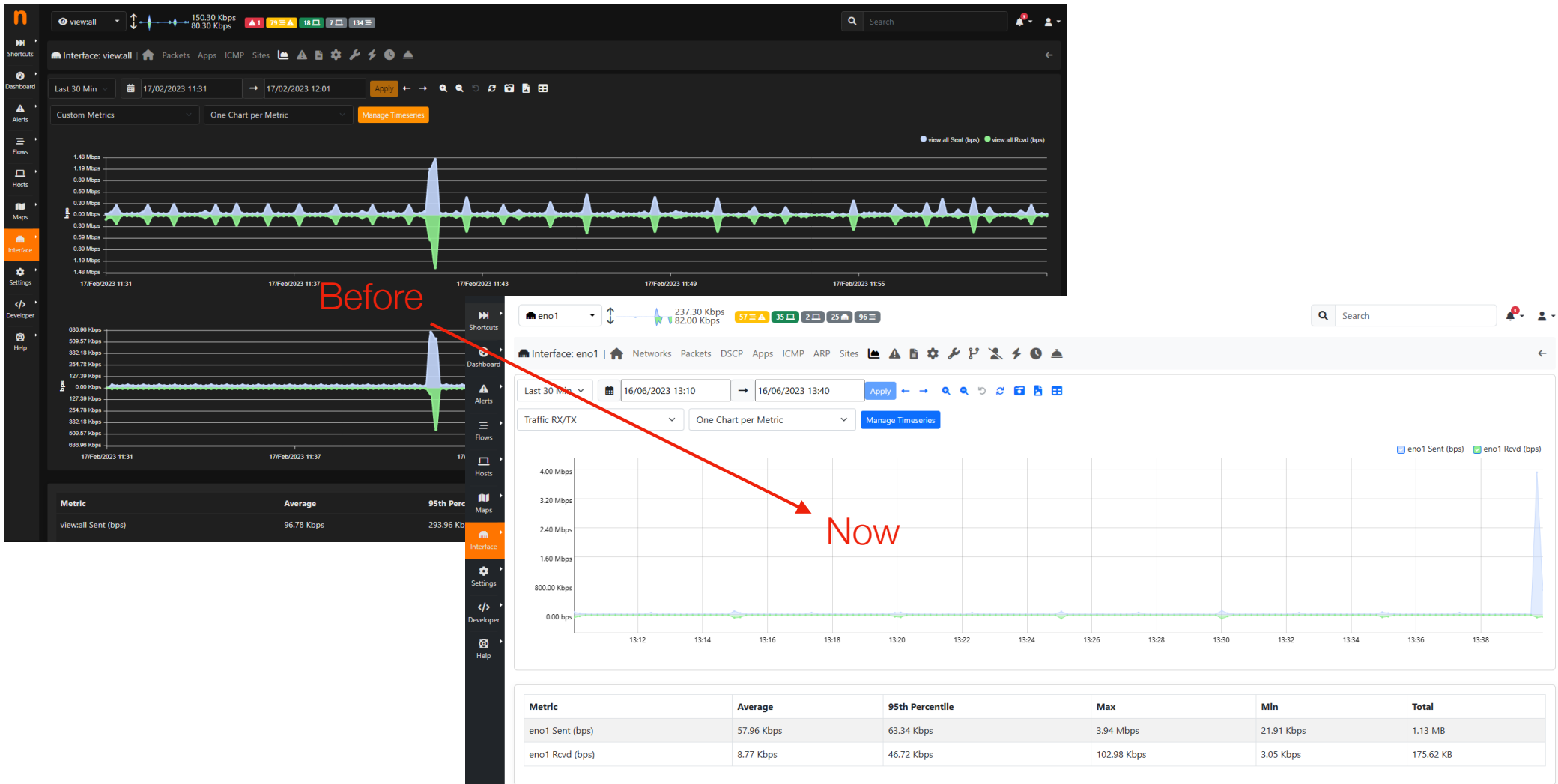
< 1 >

Host: 192.168.2.209 |

MAC Address / Device Type	94:E9:79:E4:07:7B	Unknown
First / Last Seen	06/16/2023 08:00:16 [3 Days, 07:19:16 ago]	06/16/2023 08:00:17 [3 Days, 07:19:15 ago]
IP Address / Network	192.168.2.209	192.168.2.0/24
Name	192.168.2.209	

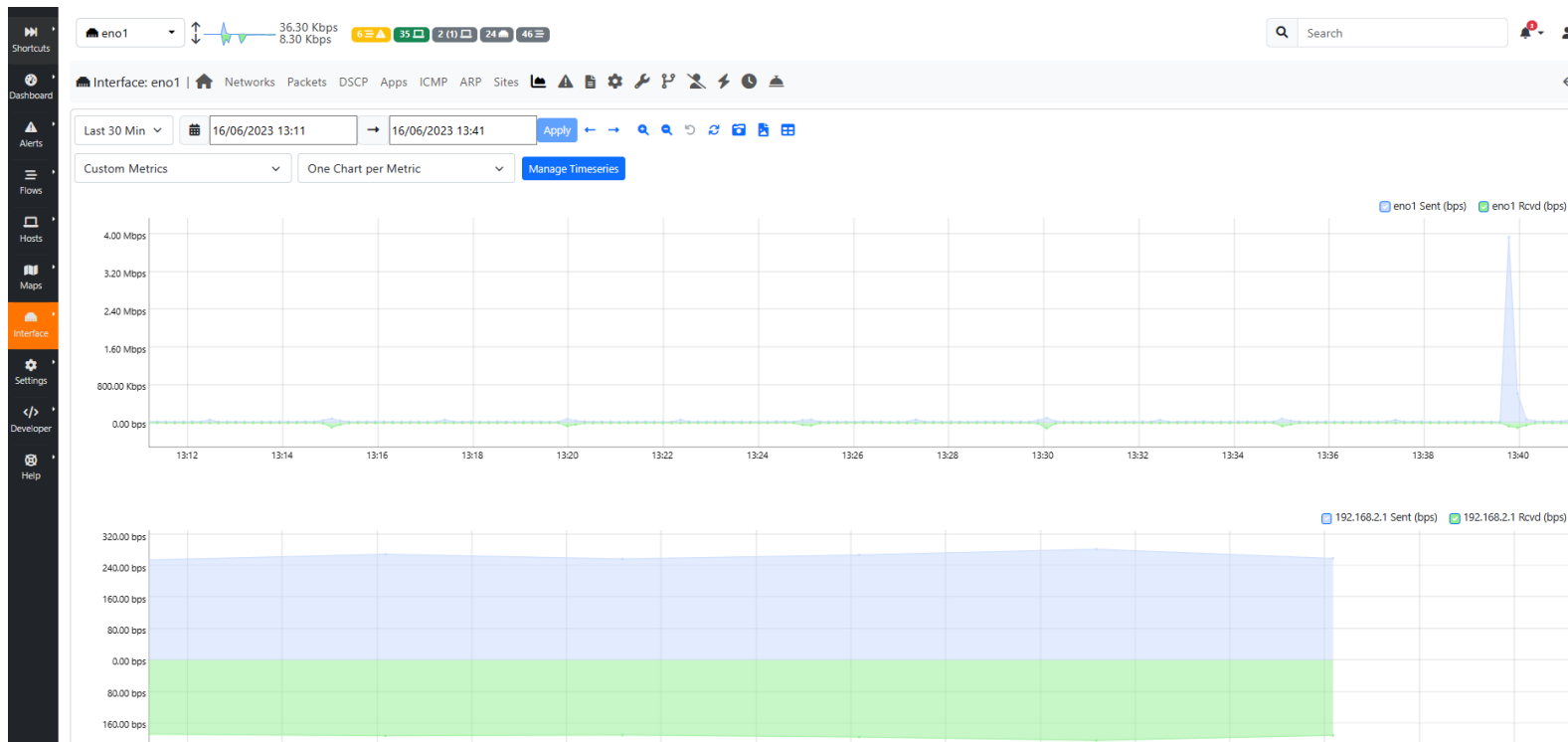
ntopng New UI

Timeseries (1/2)



Timeseries (1/2)

- Lowered loading time (4/5 s \sim > below 1 s)
- More responsive
- More user friendly



Tables Refactoring (1/3)

Historical Flows | **Flows** Analysis

Hourly Flows Last 30 Min 16/06/2023 13:14 → 16/06/2023 13:44 Apply

Filters

Show 10 Entries Top Applications Top Info Search:

Actions	Begin	End	Protocol	Application	Score	Flow	Pkts	Bytes	Thpt	Cli ASN	Srv ASN	L7 Category	Status	Flow Risk
⋮	13:40:35	13:41:49	UDP	DHCPV6 DPI		fe80::36db:fdff:fe80:d9a... 6:546 ↔ ff02::1:2:547	7 Pkts	756 Bytes	80.64 bps			Network	Normal	
⋮	13:40:55	13:40:55	UDP	DHCPV6 DPI		fe80::ec4:7aff:fecc4e6... e:546 ↔ ff02::1:2:547	1 Pkts	104 Bytes	832 bps			Network	Normal	
⋮	13:41:21	13:41:21	U											
⋮	13:41:30	13:41:30	U											

Alerts Explorer | All 1 SNMP Flow MAC Address System Active Monitoring 1 User

Past Ack Last 30 Min 16/06/2023 13:15 → 16/06/2023 13:45 Apply

Filters

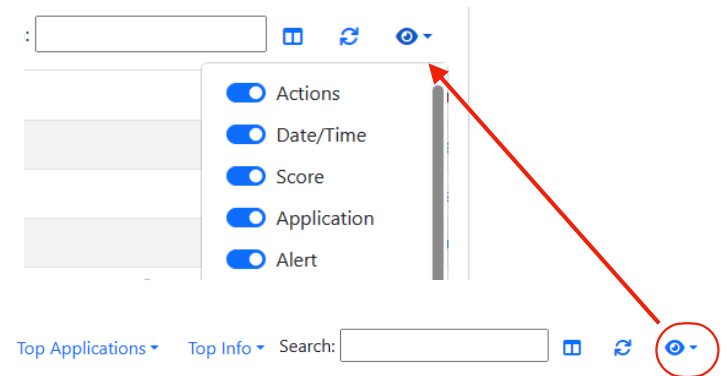
Show 10 Entries Top Clients Top Servers Top Alerts Top Applications Top Client Networks Top Server Networks Top DGA Domains Search:

Actions	Date/Time	Score	Application	Alert	Flow	Description	Com
⋮	13:40:18	10	UDP:DHCPV6 DPI	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?	1:4E
⋮	13:42:12	10	UDP:DHCPV6 DPI	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?	1:4E
⋮	13:40:14	10	UDP:NetBIOS.SMBv1 ...	Periodic Flow	192.168.2.98:138 ↔ 192.168.2.255:138	Periodic Flow ?	1:70
⋮	13:39:51	60	TCP:HTTP.ntop DPI	Known Proto on Non Std Port	192.168.2.153:60622 ↔ devel:3001	Known Proto on Non Std Port ?	1:ksE
⋮	13:39:52	60	TCP:HTTP.ntop DPI	Known Proto on Non Std Port	192.168.2.153:60623 ↔ devel:3001	Known Proto on Non Std Port ?	1:Oh
⋮	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60627 ↔ devel:3001	Known Proto on Non Std Port ?	1:pw



Tables Refactoring (2/3)

- Reworked tables (homeproduct)
- Hastened loading
- Change the length of columns
- Remove/Add columns



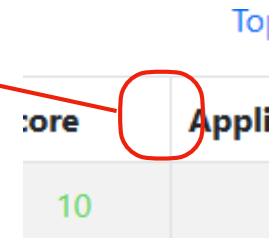
Show 10 Entries

Top Applications ▾ Top Info ▾ Search:

Actions	Begin	End	Protocol	Application	Score	Flow	Pkts	Bytes	Thpt	Cli ASN	Srv ASN	L7 Category	Status	Flow Risk
	13:40:35	13:41:49	UDP	DHCPV6 DPI		fe80::36db:fdff:fe80:d9a... 6:546 ↔ ff02::1:2:547	7 Pkts	756 Bytes	80.64 bps			Network	Normal	
	13:40:55	13:40:55	UDP	DHCPV6 DPI		fe80::ec4:7aff:fecc:4e6... e:546 ↔ ff02::1:2:547	1 Pkts	104 Bytes	832 bps			Network	Normal	
	13:41:21	13:41:21	UDP	DHCPV6 DPI		fe80::ec4:7aff:fecc:4c5... 3:546 ↔ ff02::1:2:547	1 Pkts	98 Bytes	784 bps			Network	Normal	
	13:41:30	13:41:30	UDP	DHCPV6 DPI		fe80::20c:29ff:fe96:455... c:546 ↔ ff02::1:2:547	1 Pkts	104 Bytes	832 bps			Network	Normal	
	13:41:48	13:41:48	IGMP	IGMP		192.168.1.2 ↔ 224.0.0.251	2 Pkts	120 Bytes	960 bps			Network	Normal	
	13:41:12	13:41:12	UDP	Unknown		192.168.2.106:5678 ↔ broadcast:5678	1 Pkts	219 Bytes	1.75 kbps			Unspecified	Normal	
	13:41:50	13:41:50	IGMP	IGMP		192.168.2.134 ↔ 224.0.0.251	2 Pkts	120 Bytes	960 bps			Network	Normal	

Tables Refactoring (3/3)

Click between columns and you can change the length of the columns



Actions	Date/Time	Score	Application	Alert	Flow	Description	Community ID
☰	13:40:18	10	UDP:DHCPV6 DPI	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?	1:4EaXWqS7ipjwI
☰	13:42:12	10	UDP:DHCPV6 DPI	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?	1:4EaXWqS7ipjwI
☰	13:40:14	10	UDP:NetBIOS.SMBv1 DPI	Periodic Flow	192.168.2.98:138 ↔ 192.168.2.255:138	Periodic Flow ?	1:70CqD4CQDAIt+
☰	13:39:51	60	TCP:HTTP.ntop DPI	Known Proto on Non Std Port	192.168.2.153:60622 ↔ devel:3001	Known Proto on Non Std Port ?	1:ksEOkZ0R4ppj/z
☰	13:39:52	60	TCP:HTTP.ntop DPI	Known Proto on Non Std Port	192.168.2.153:60623 ↔ devel:3001	Known Proto on Non Std Port ?	1:OhKxNyUOMIL9
☰	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60627 ↔ devel:3001	Known Proto on Non Std Port ?	1:pw5kWo459QG+
☰	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60628 ↔ devel:3001	Known Proto on Non Std Port ?	1:sVh3OHEU7cEtG
☰	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60630 ↔ devel:3001	Known Proto on Non Std Port ?	1:w/3dy9whiLBigw
☰	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60626 ↔ devel:3001	Known Proto on Non Std Port ?	1:nJBHtWzOIXqqsI
☰	13:39:52	60	TCP:HTTP DPI	Known Proto on Non Std Port	192.168.2.153:60629 ↔ devel:3001	Known Proto on Non Std Port ?	1:iHfCpJLxe4P/856

Actions	Date/Time	Score	Application	Alert	Flow	Description
☰	13:40:18	10	UDP:DHCP...	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?
☰	13:42:12	10	UDP:DHCP...	Periodic Flow	fe80::20c:29ff:fe37:d0... 5:546 ↔ ff02::1:2:547	Periodic Flow ?
☰	13:40:14	10	UDP:NetBI...	Periodic Flow	192.168.2.98:138 ↔ 192.168.2.255:138	Periodic Flow ?
☰	13:39:51	60	TCP:HTTP....	Known Proto on Non Std Port	192.168.2.153:60622 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP....	Known Proto on Non Std Port	192.168.2.153:60623 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP ...	Known Proto on Non Std Port	192.168.2.153:60627 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP ...	Known Proto on Non Std Port	192.168.2.153:60628 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP ...	Known Proto on Non Std Port	192.168.2.153:60630 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP ...	Known Proto on Non Std Port	192.168.2.153:60626 ↔ devel:3001	Known Proto on Non Std Port ?
☰	13:39:52	60	TCP:HTTP ...	Known Proto on Non Std Port	192.168.2.153:60629 ↔ devel:3001	Known Proto on Non Std Port ?

Smart Recording

Continuous Recording

- In most cases it's not possible to predict when a network event occurs
- In order to drill down up to the packet level:
 - We need to record traffic 24/7
 - On-demand capture is not an option



Data Retention

- Data retention depends on traffic rate and storage size
- Example:

Traffic rate	10 Gbps
Data on disk	1,2 GB/s
Data on disk	4 TB/h
Data on disk	100 TB/day

- 10x at 100 Gbps

Saving Space

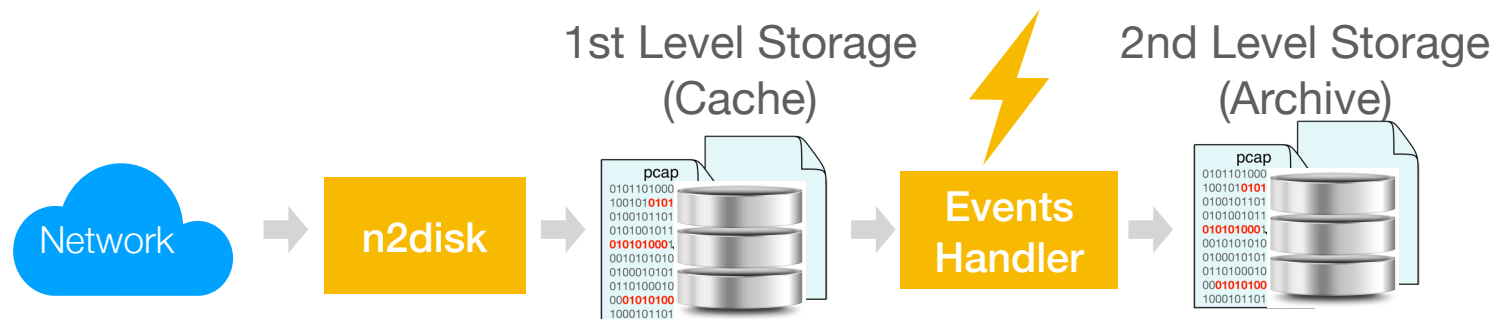
- Packet compression: save up to 5% on Internet traffic (more on LAN traffic)
- Packet slicing: good if interested in headers only
- BPF filtering: difficult to predict
- L7 filtering: good to discard or shunt unwanted traffic (e.g. encrypted, compressed, multimedia)

Not all traffic is alike

- What if our storage does not satisfy the desired data retention, even after filtering?
- Assumption: traffic matching Network events is more important than the rest of the traffic
- What we need is:
 - Prioritize selected traffic (e.g. security alerts)
 - Smart data recycling: delete traffic which is not matching any event first

Smart Data Retention

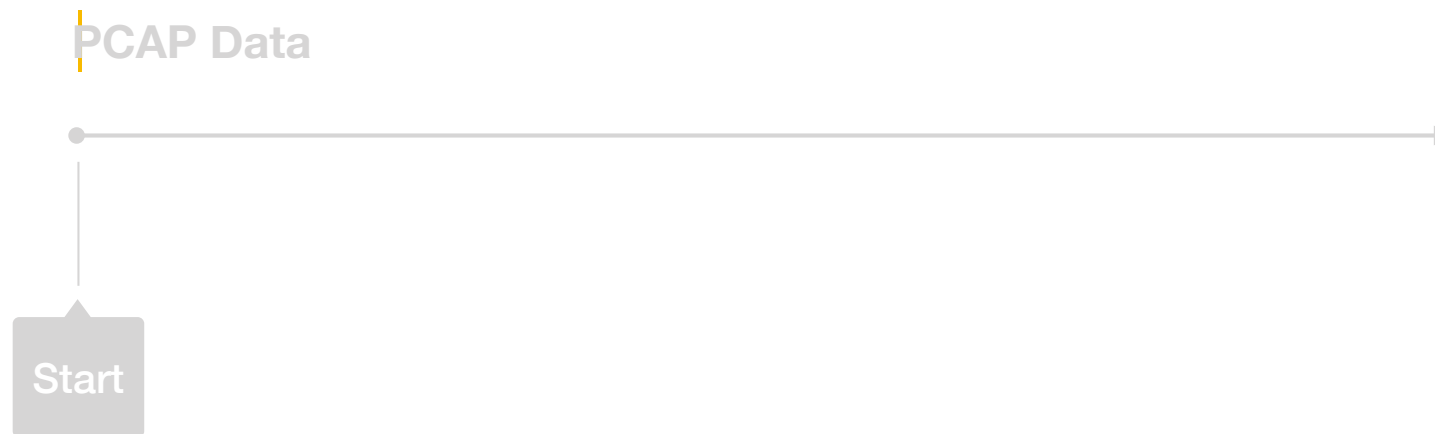
- Process Network events generated by ntopng
- Use a 1st level storage to implement continuous recording with a short data retention (cache)
- Use a 2nd level storage to archive traffic for Network events with a longer data retention (archive)



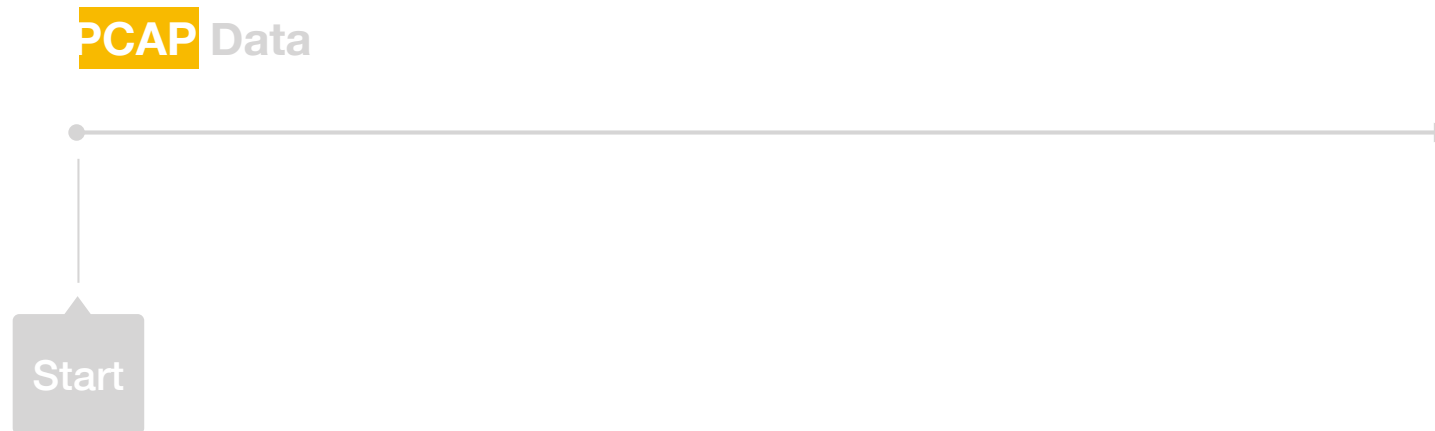
Continuous Recording



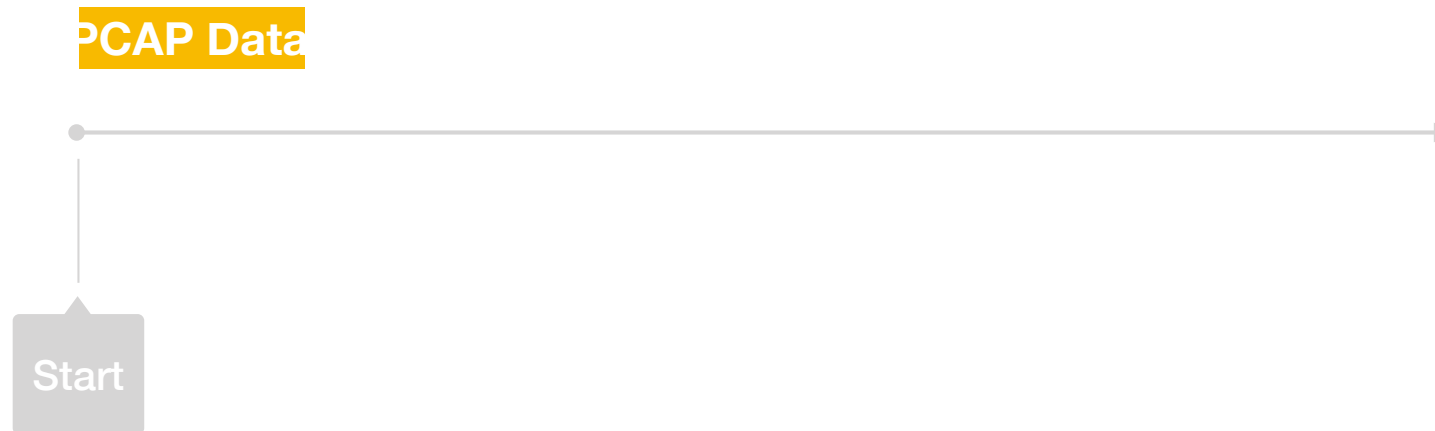
Continuous Recording



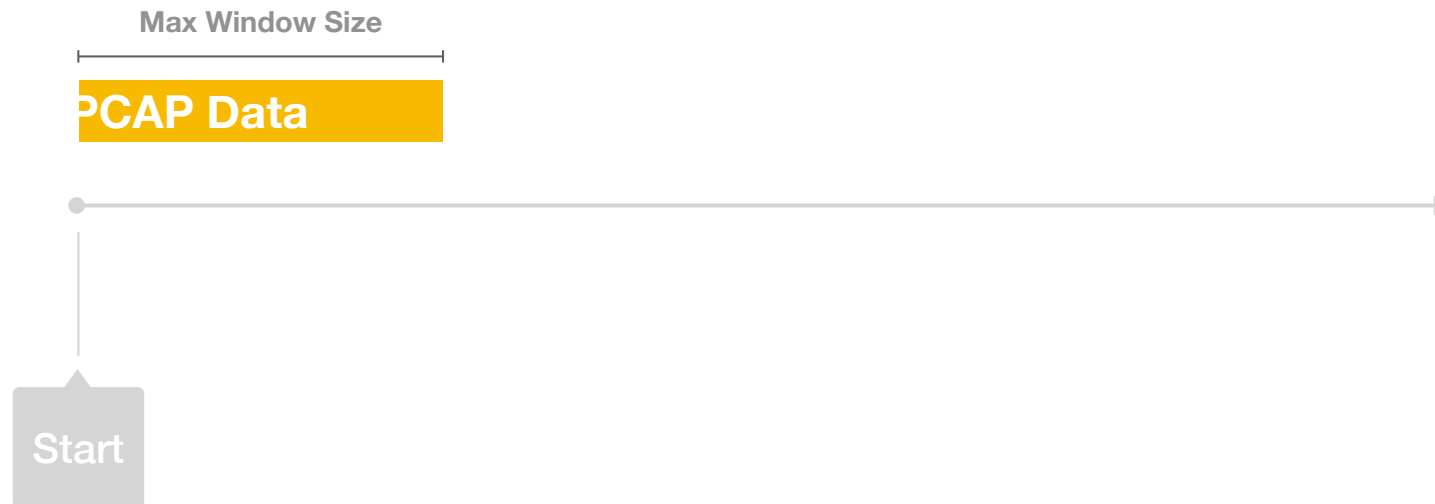
Continuous Recording



Continuous Recording



Continuous Recording



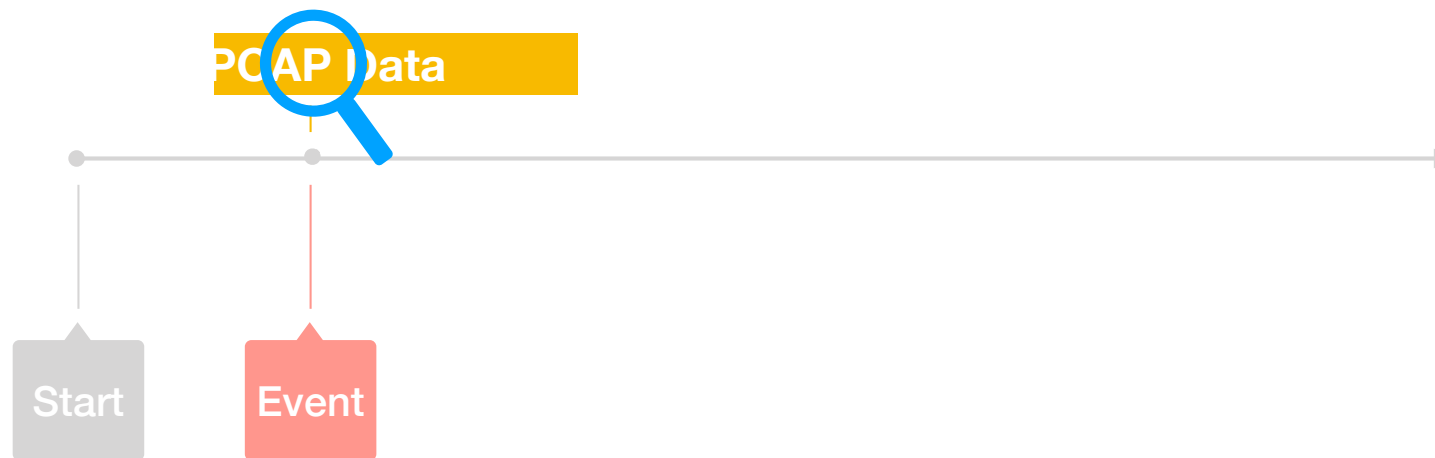
Continuous Recording



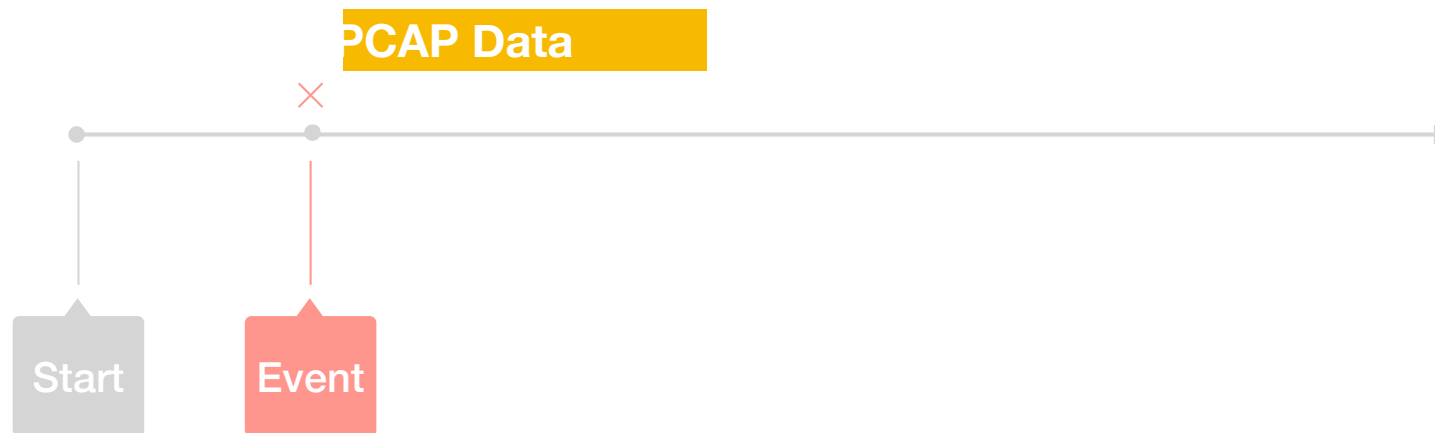
Continuous Recording



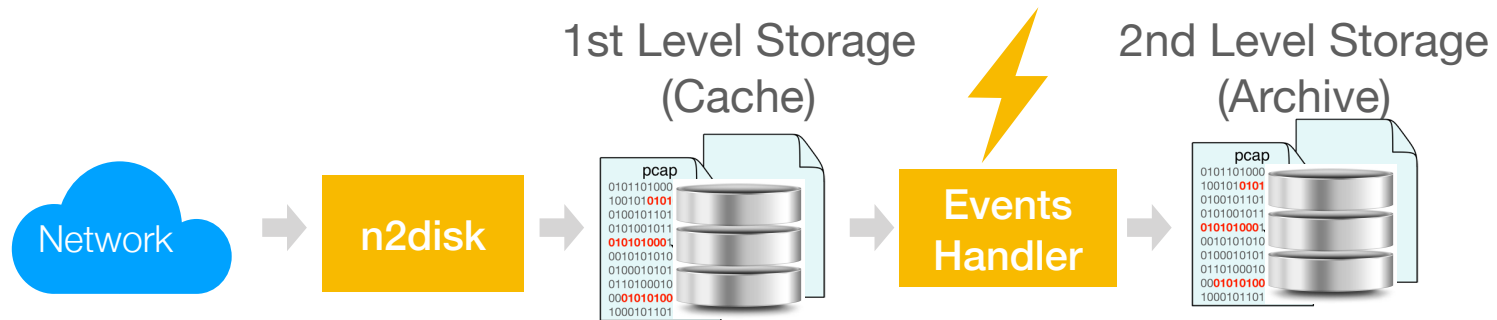
Continuous Recording



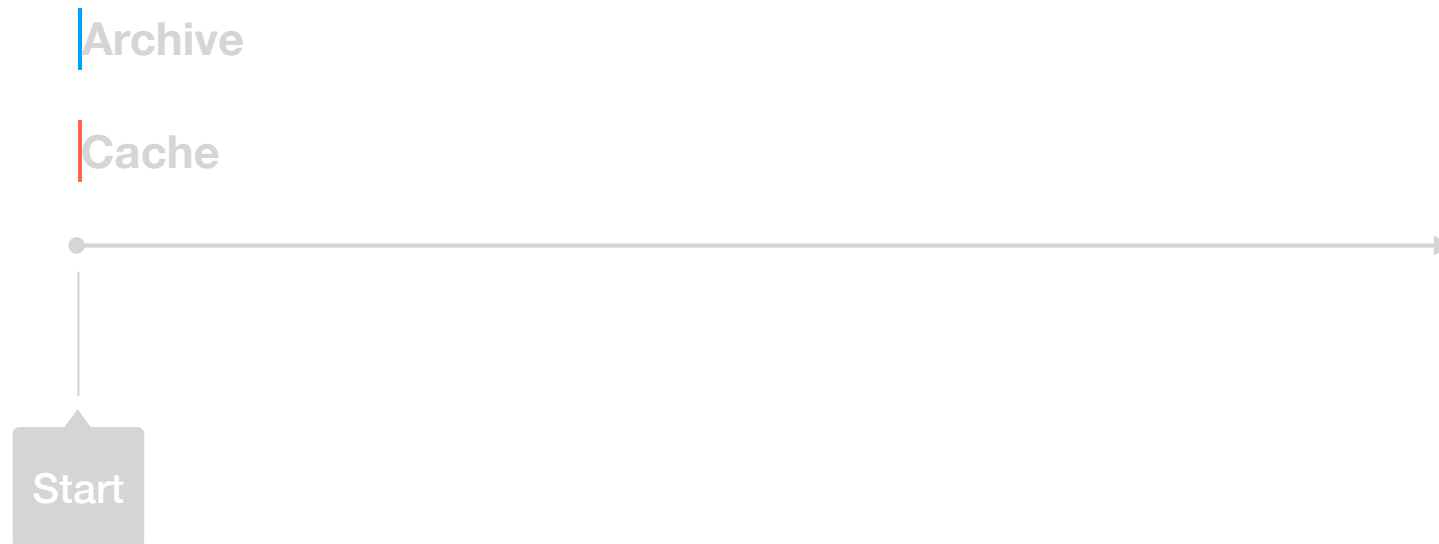
Continuous Recording



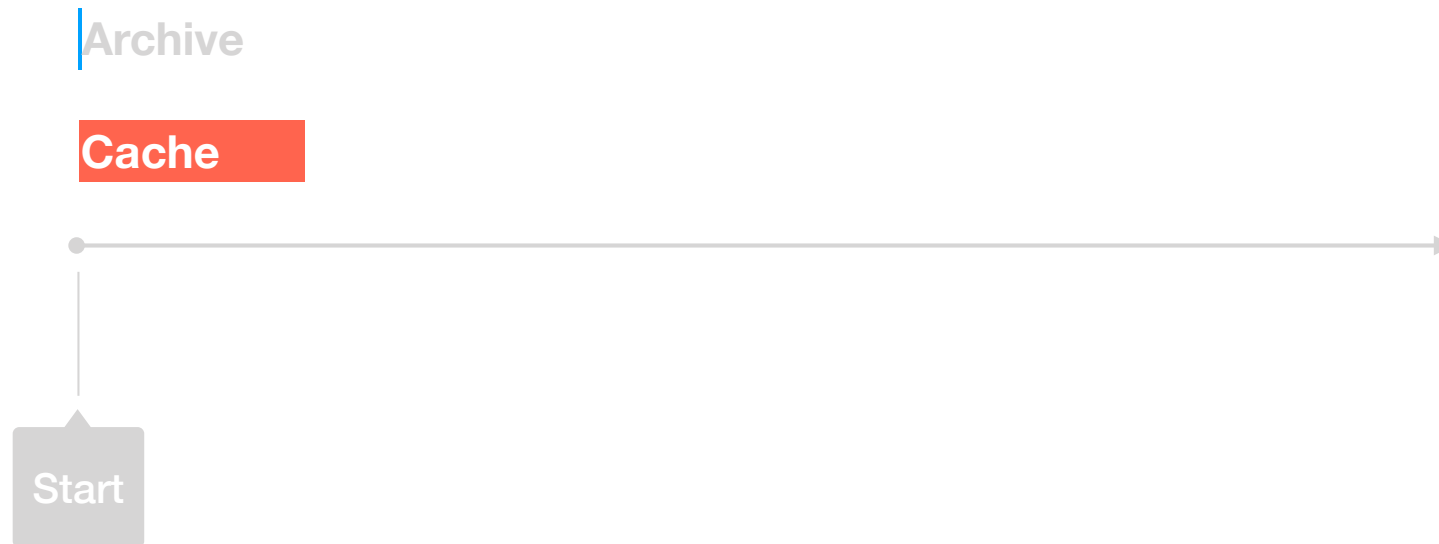
Smart Recording



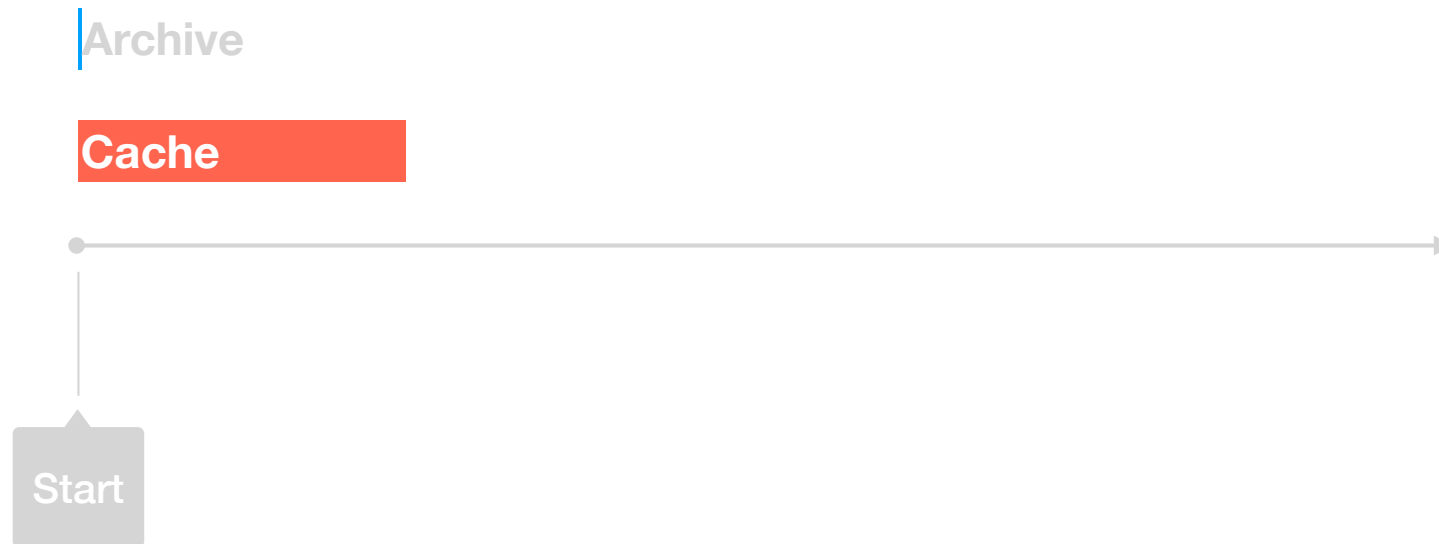
Smart Recording



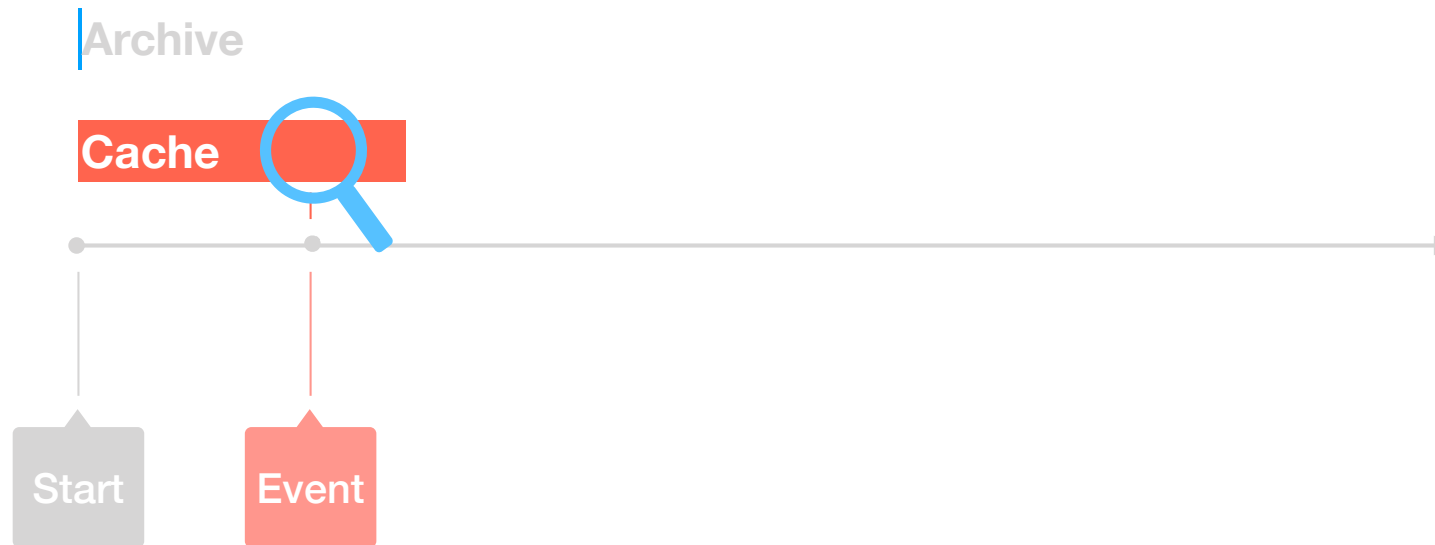
Smart Recording



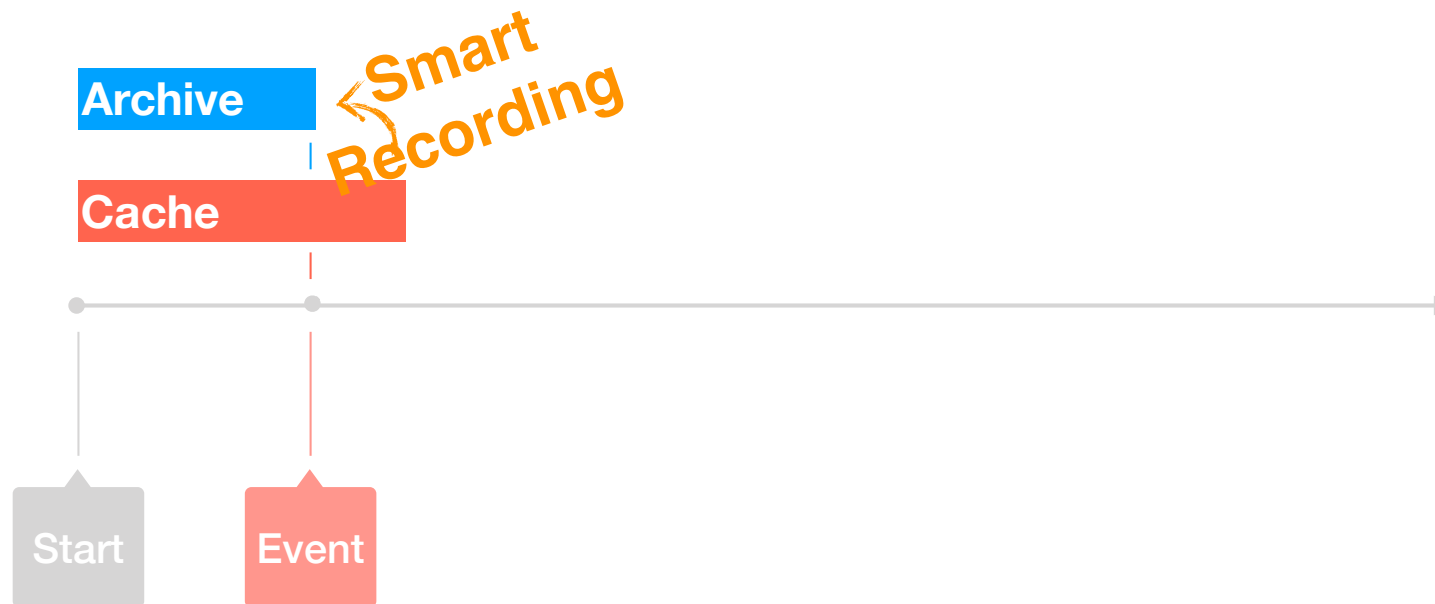
Smart Recording



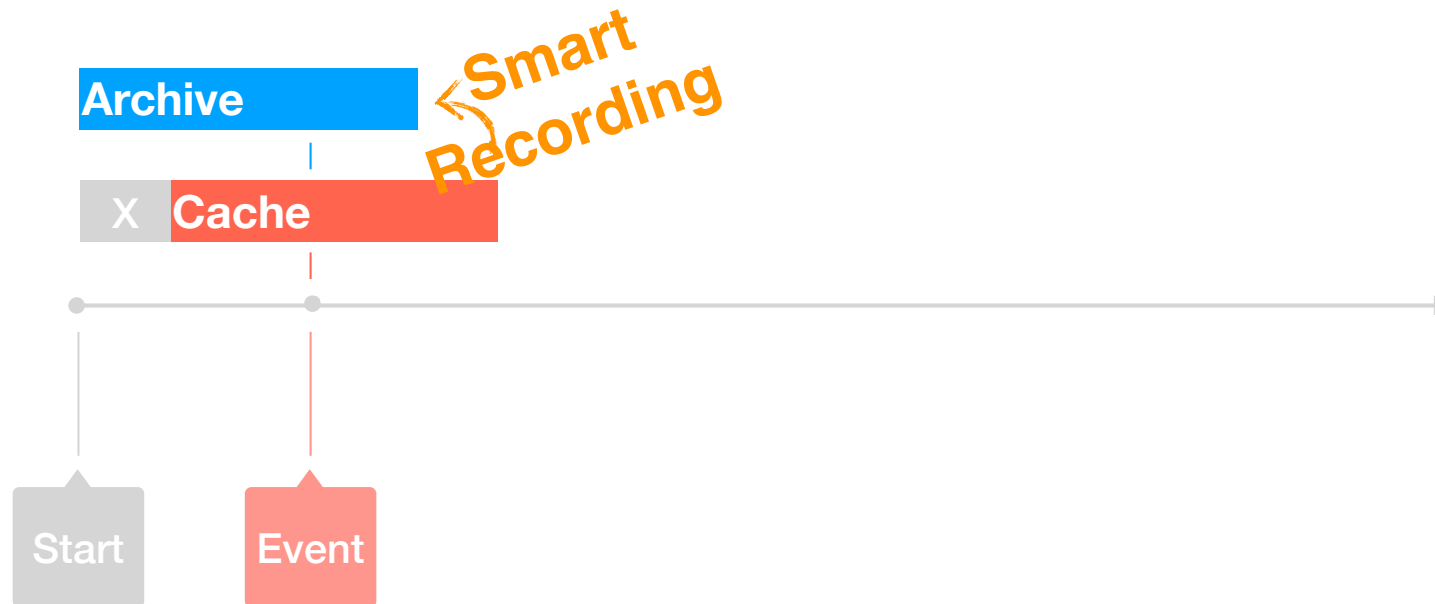
Smart Recording



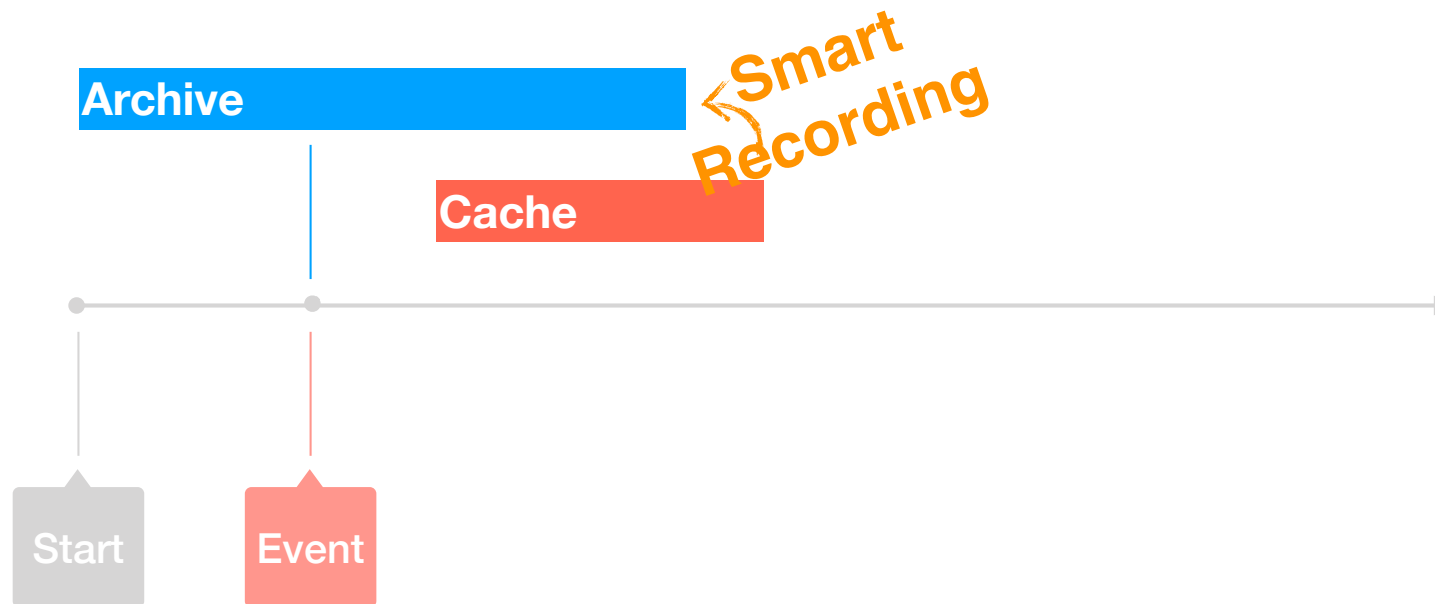
Smart Recording



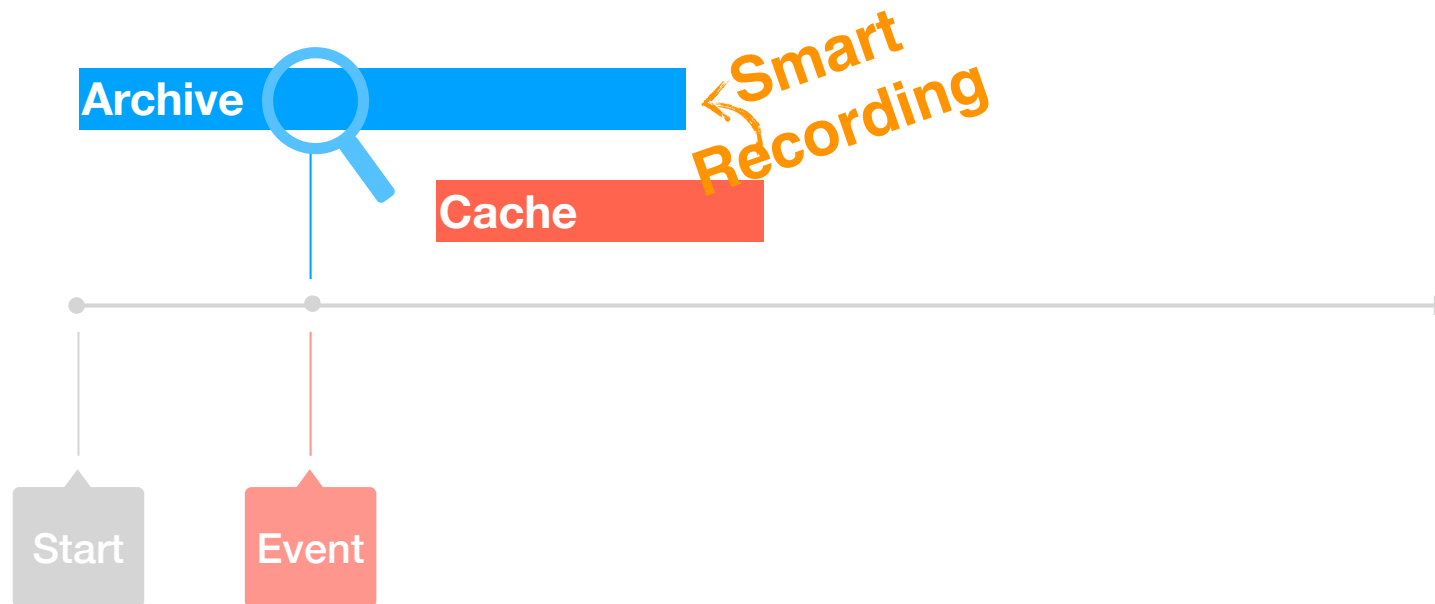
Smart Recording



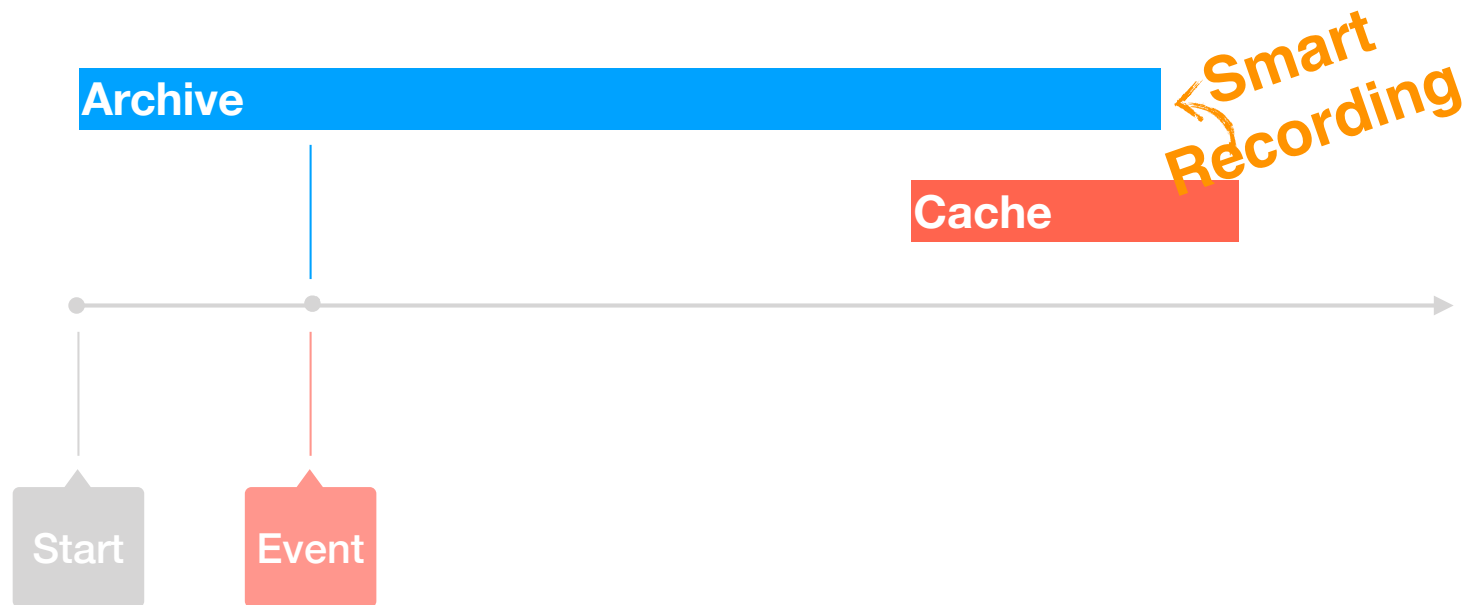
Smart Recording



Smart Recording



Smart Recording



Smart Recording

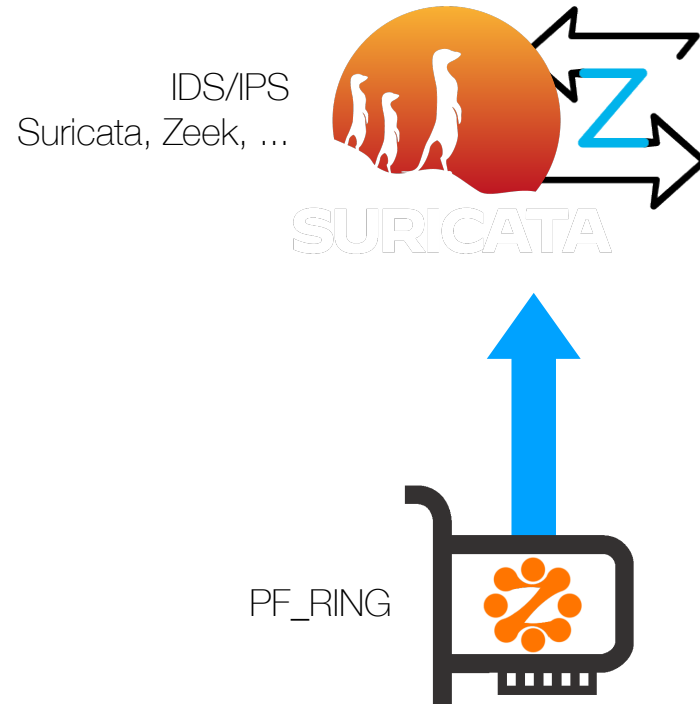


Suricata and Zeek at 100 Gbit

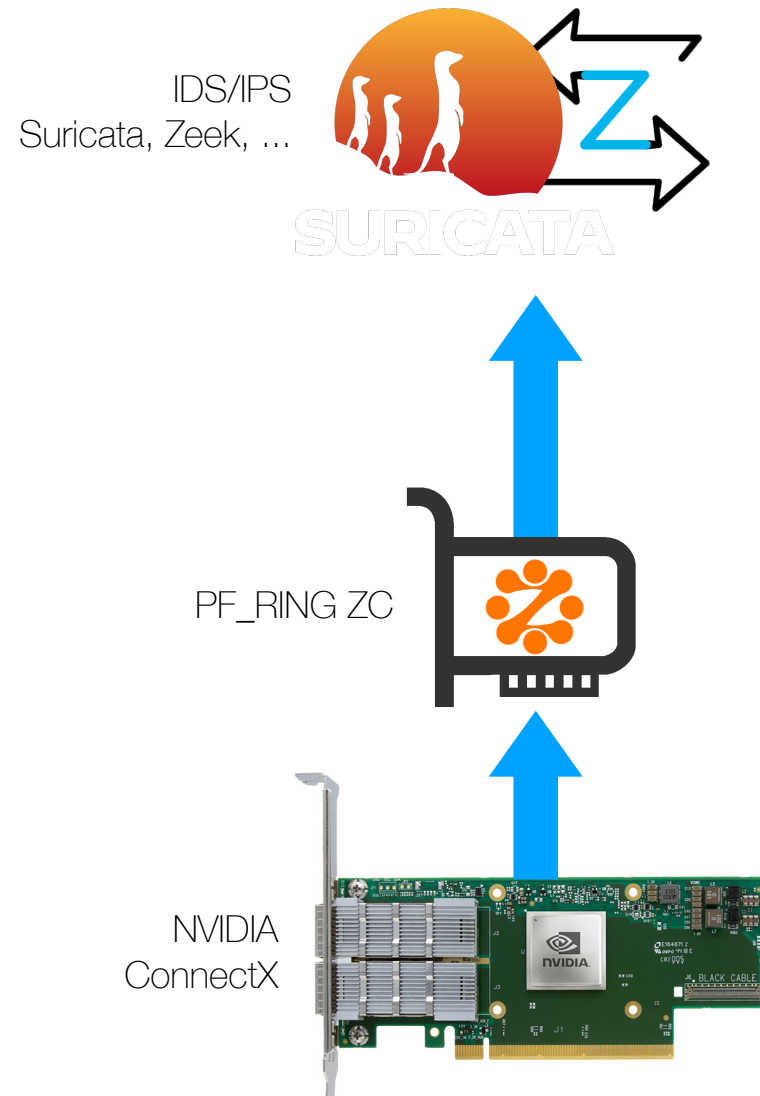
IDS Acceleration



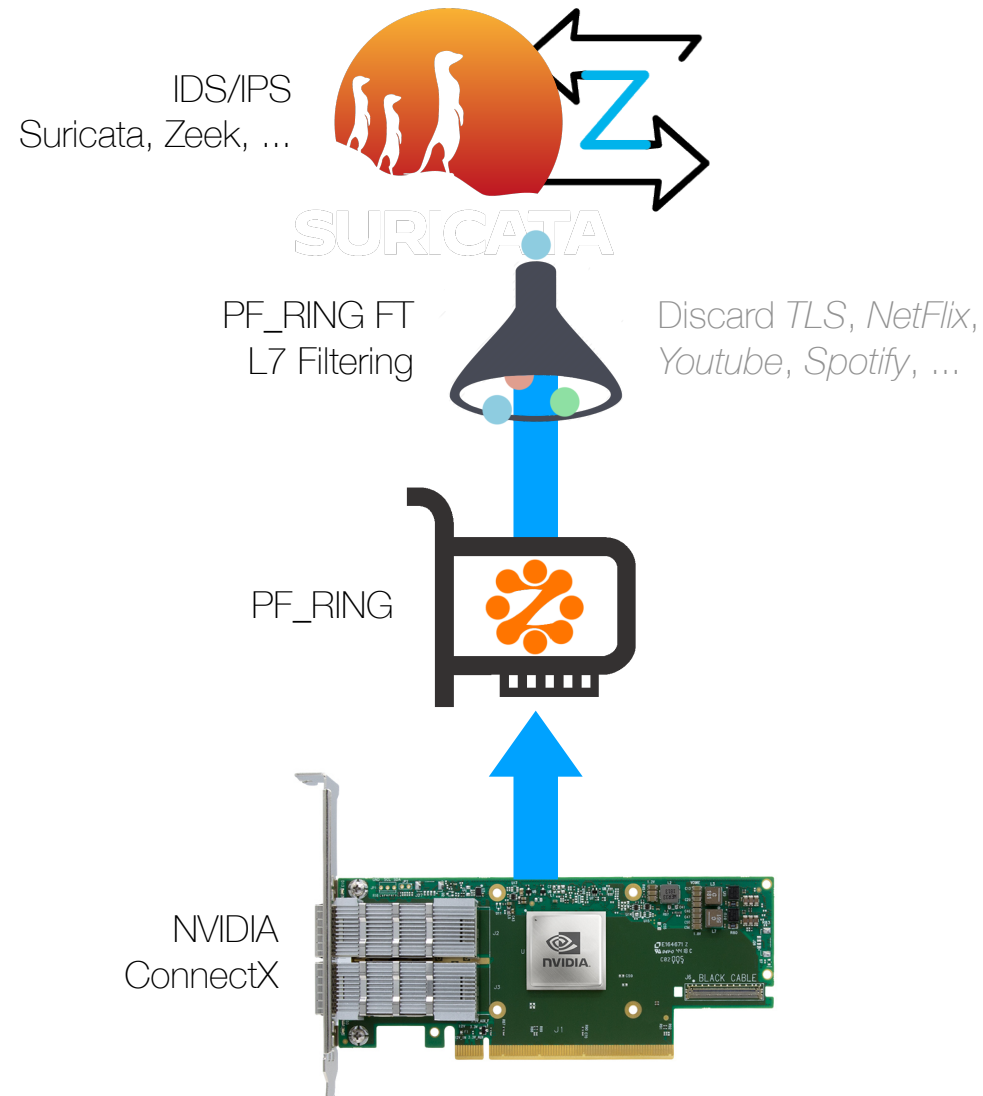
IDS Acceleration



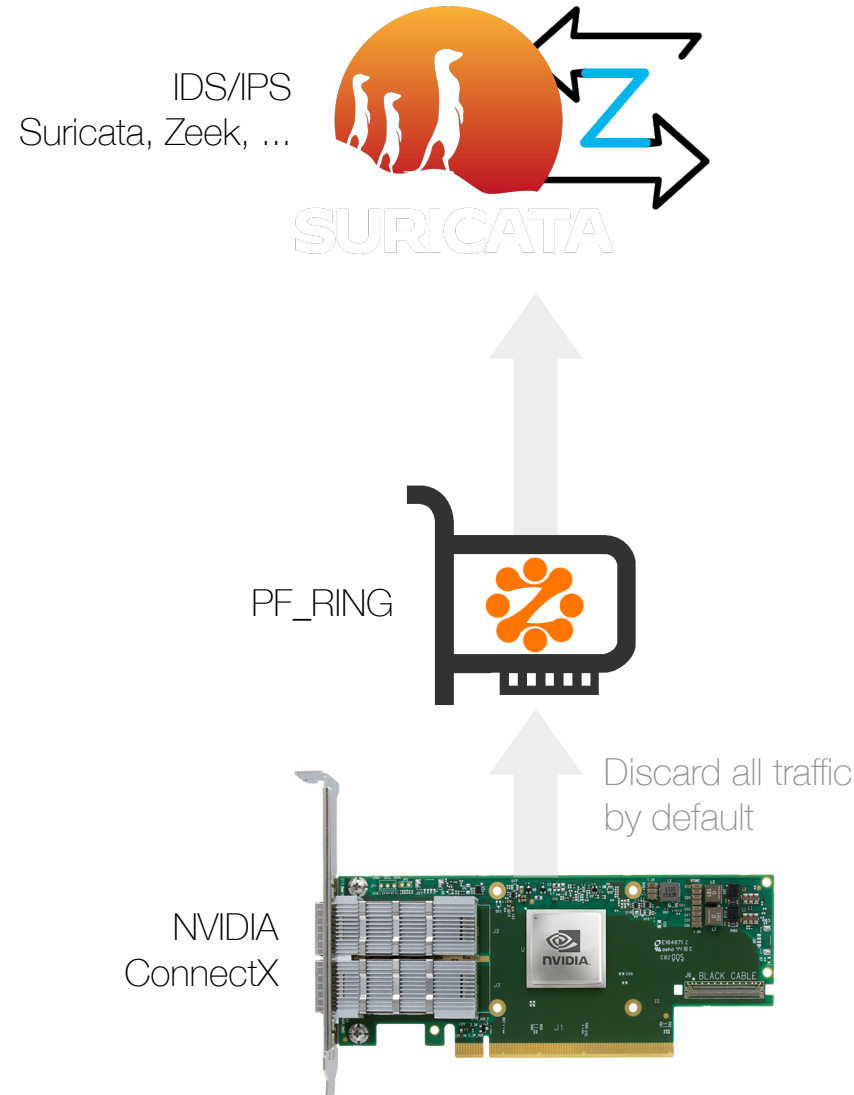
IDS Acceleration



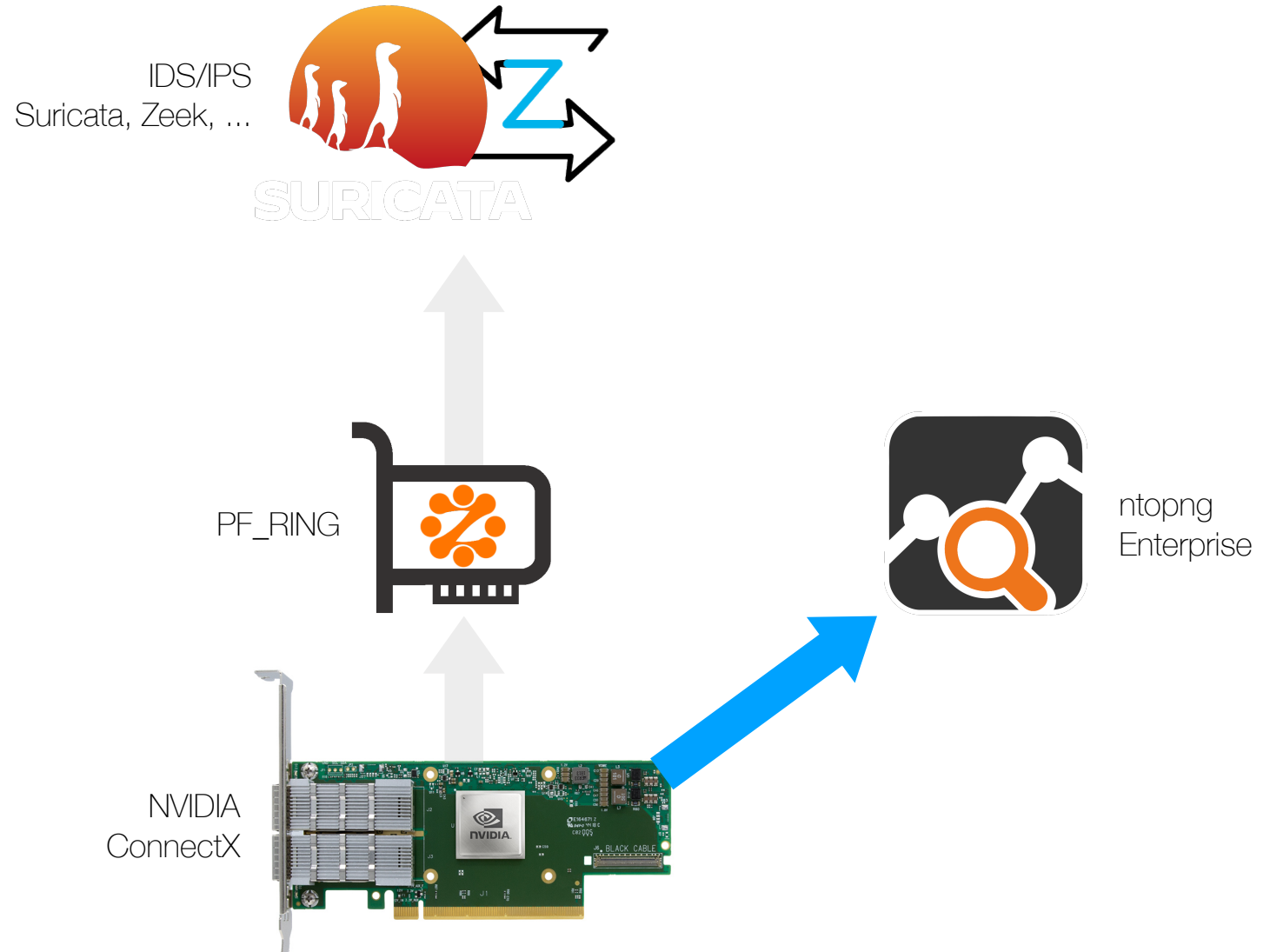
IDS Acceleration



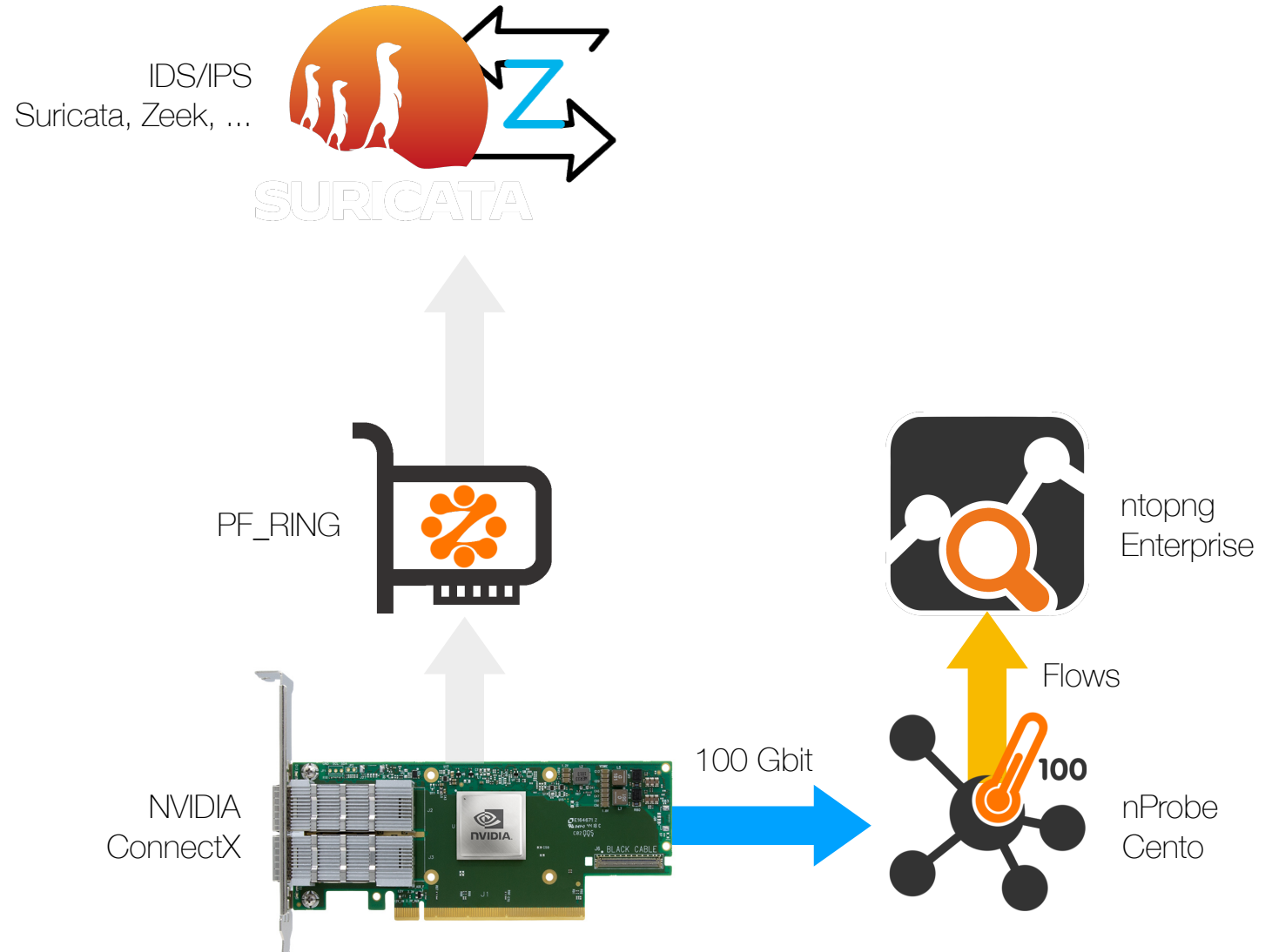
Suricata and Zeek On Demand



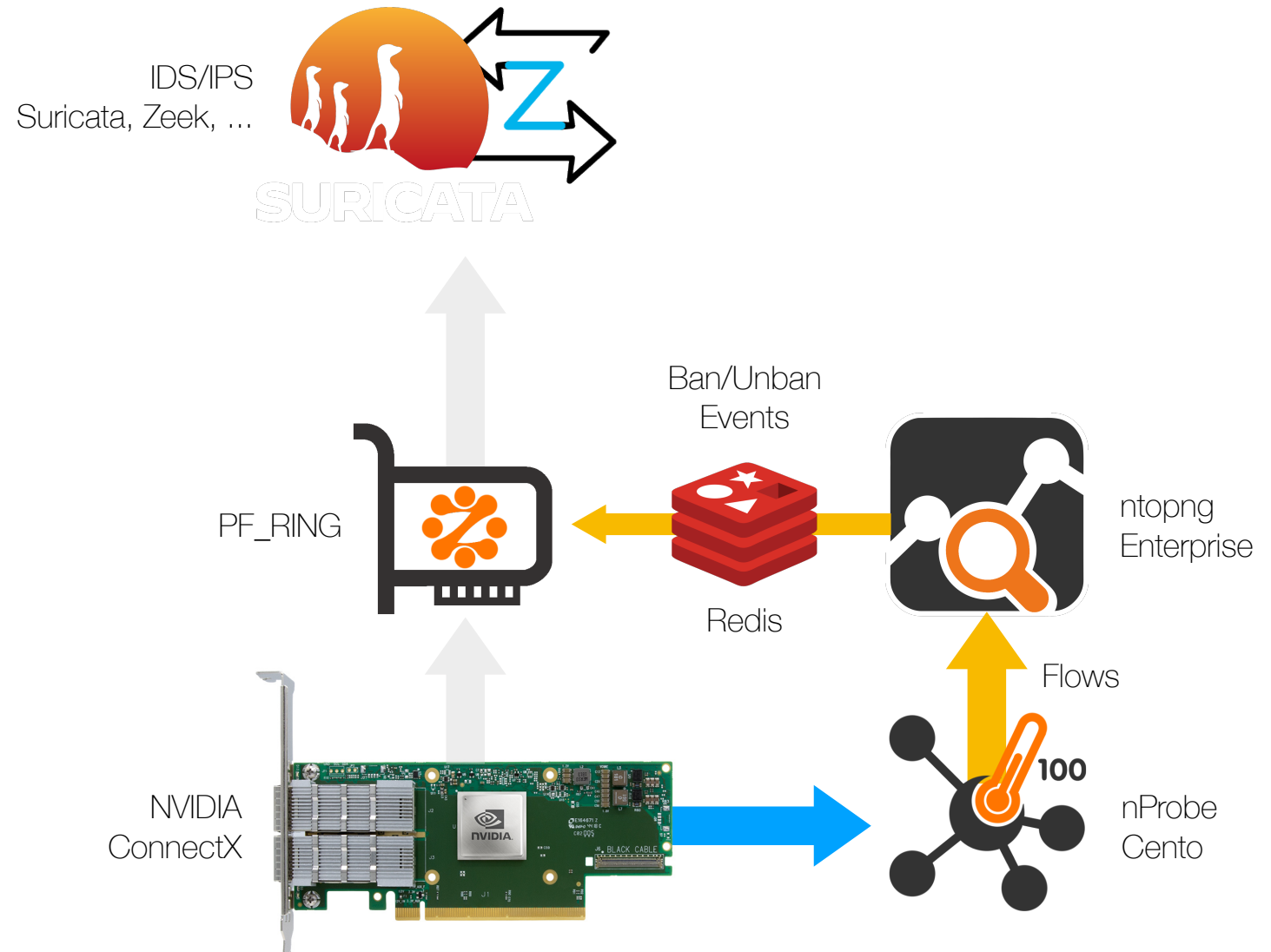
Suricata and Zeek On Demand



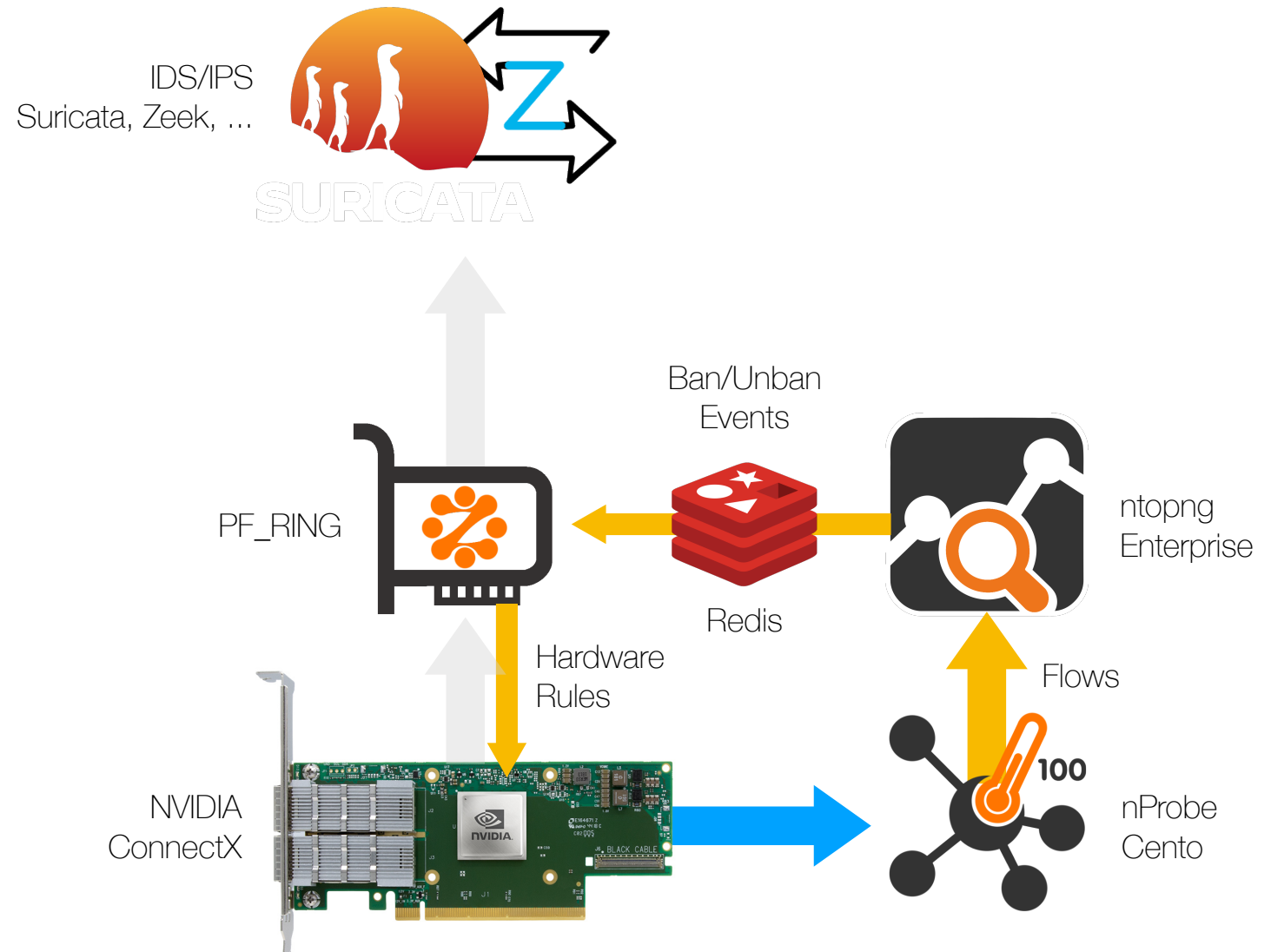
Suricata and Zeek On Demand



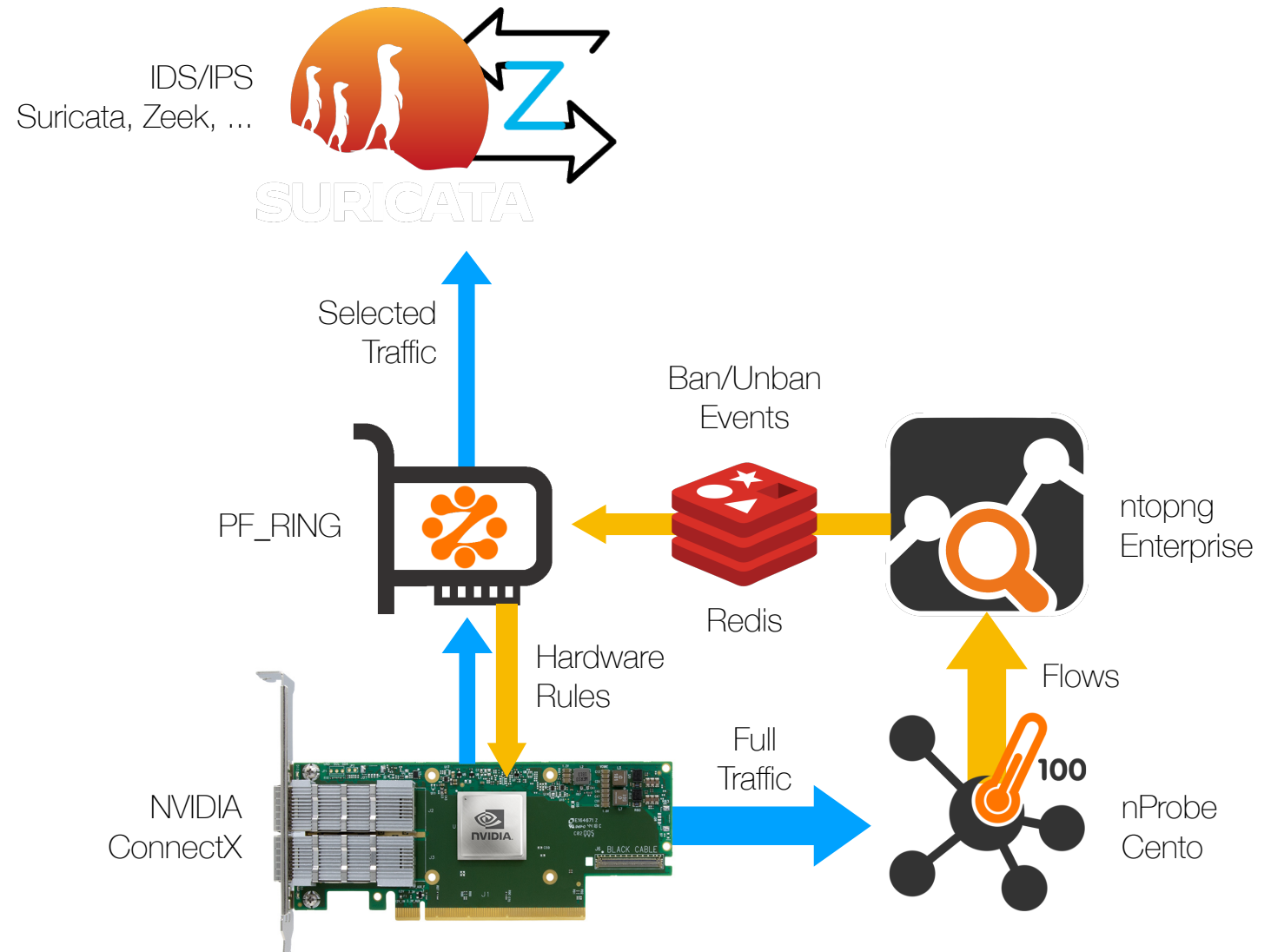
Suricata and Zeek On Demand



Suricata and Zeek On Demand

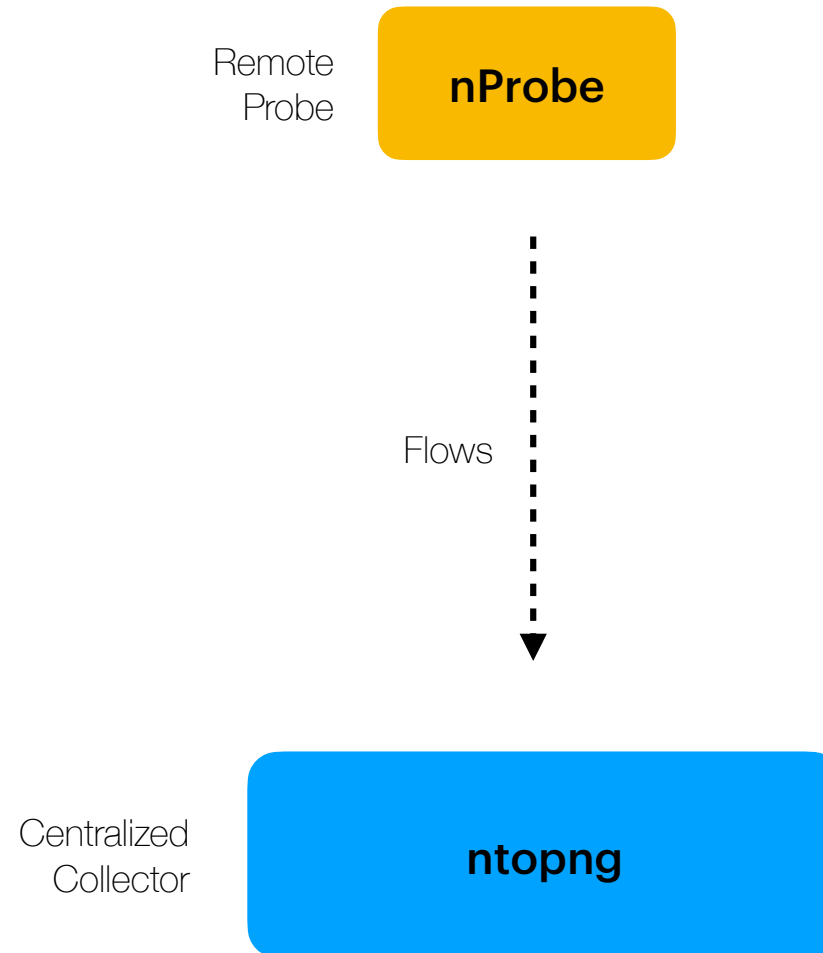


Suricata and Zeek On Demand

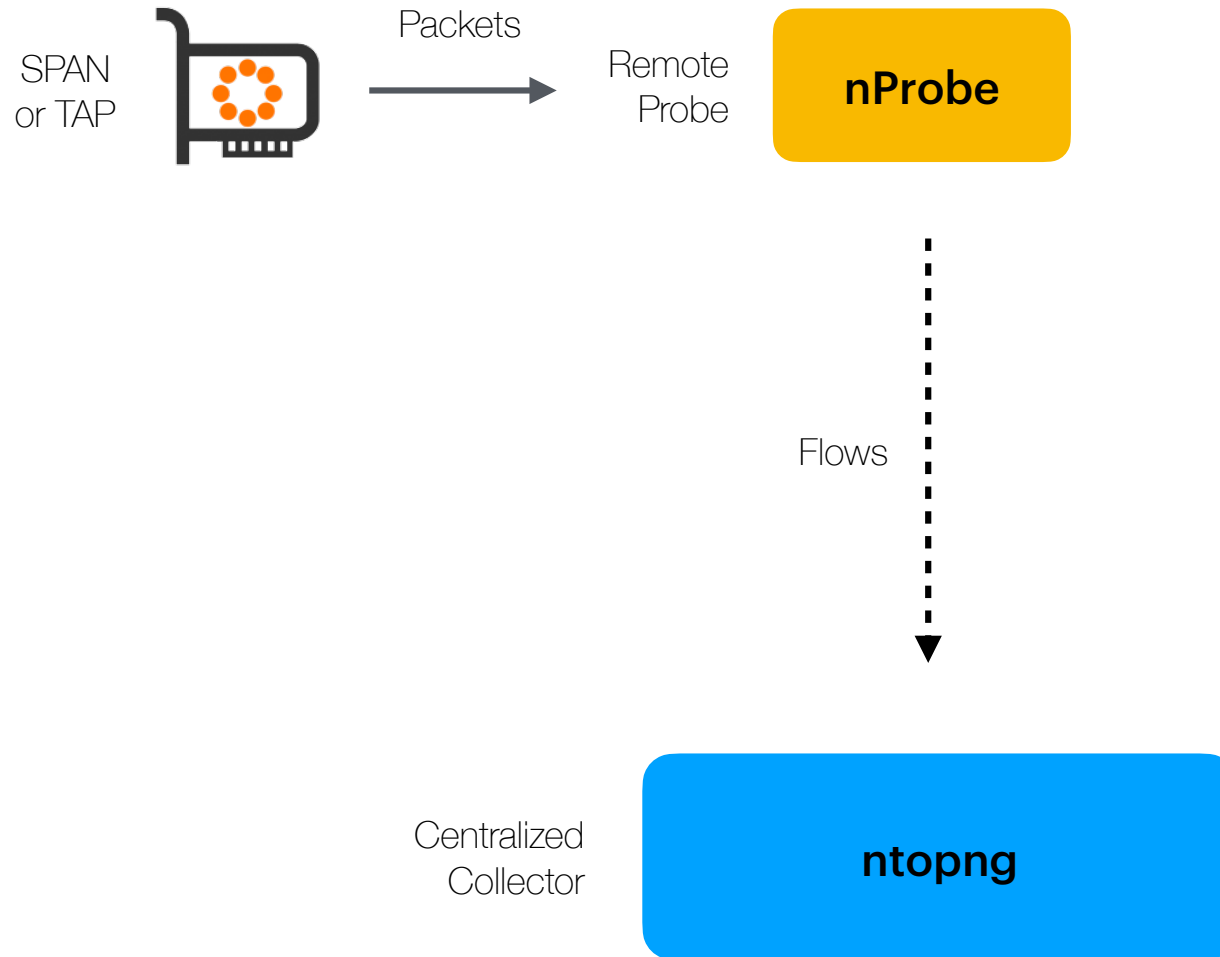


Cloud License

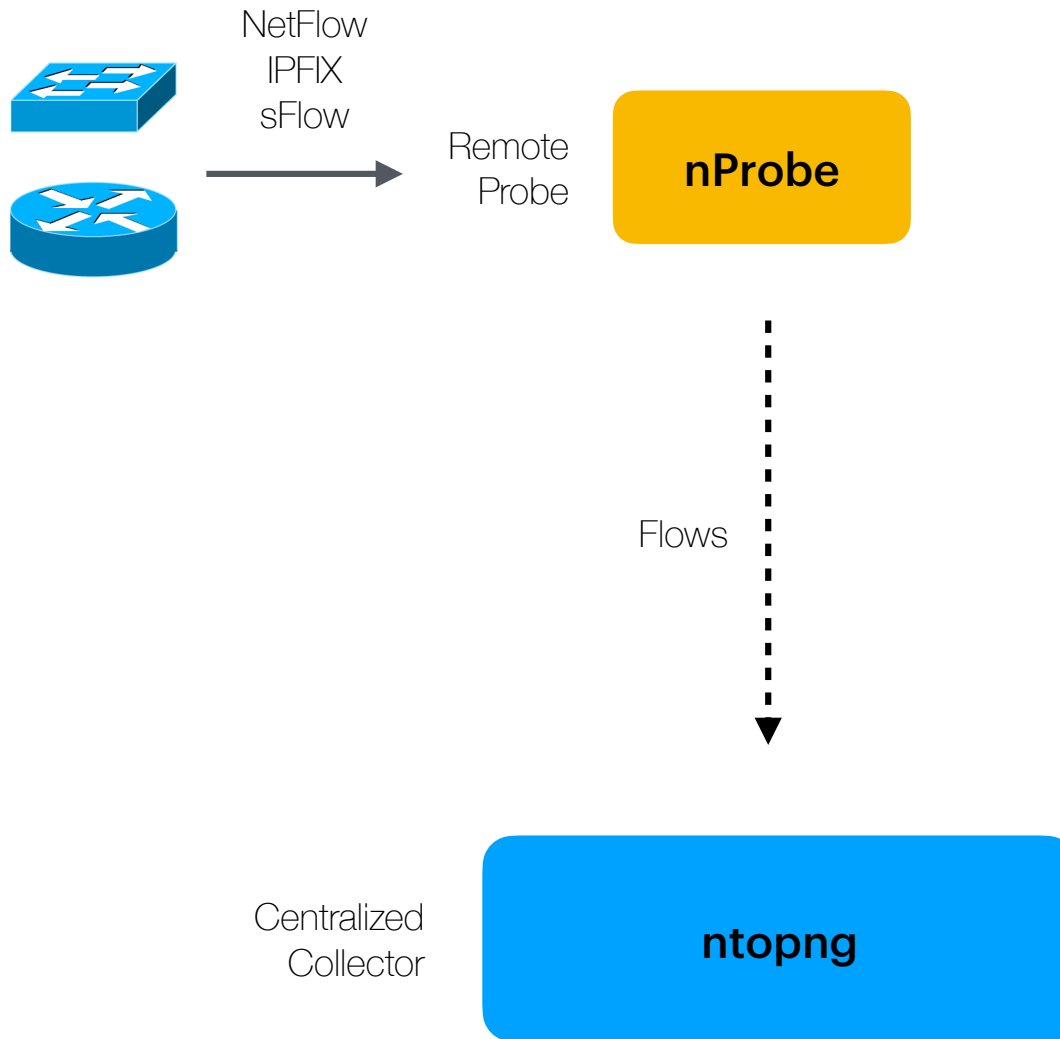
Remote Traffic Analysis



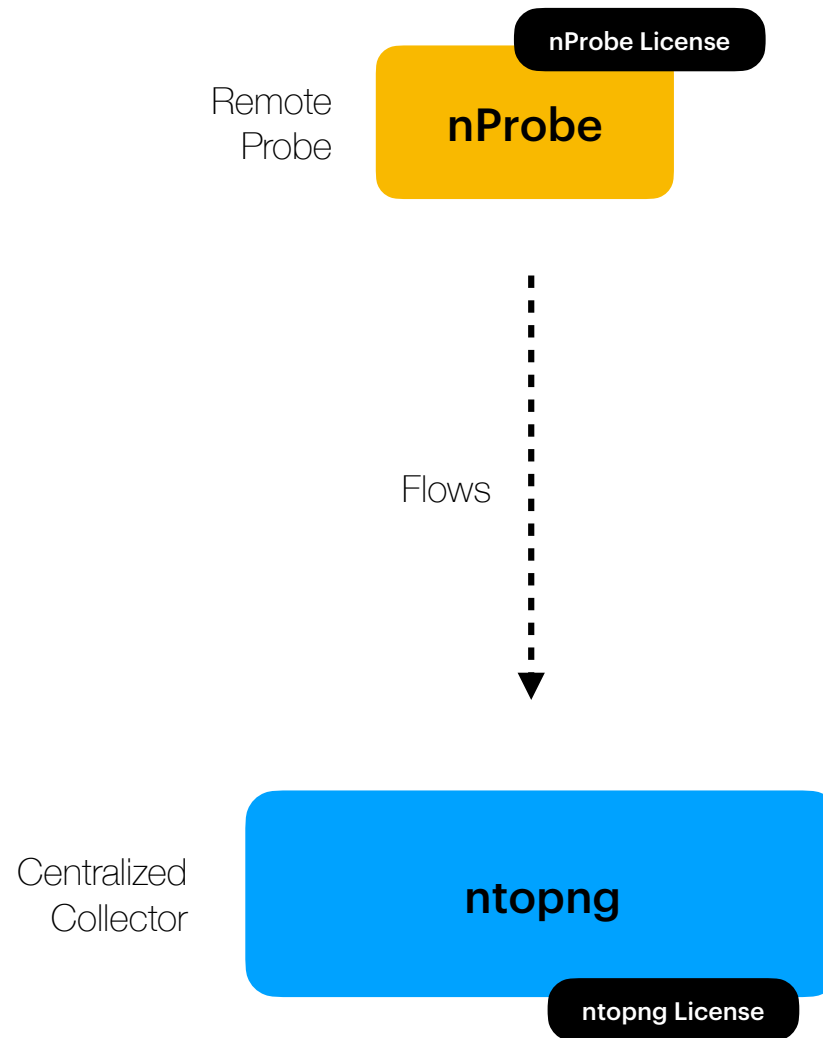
Remote Traffic Analysis



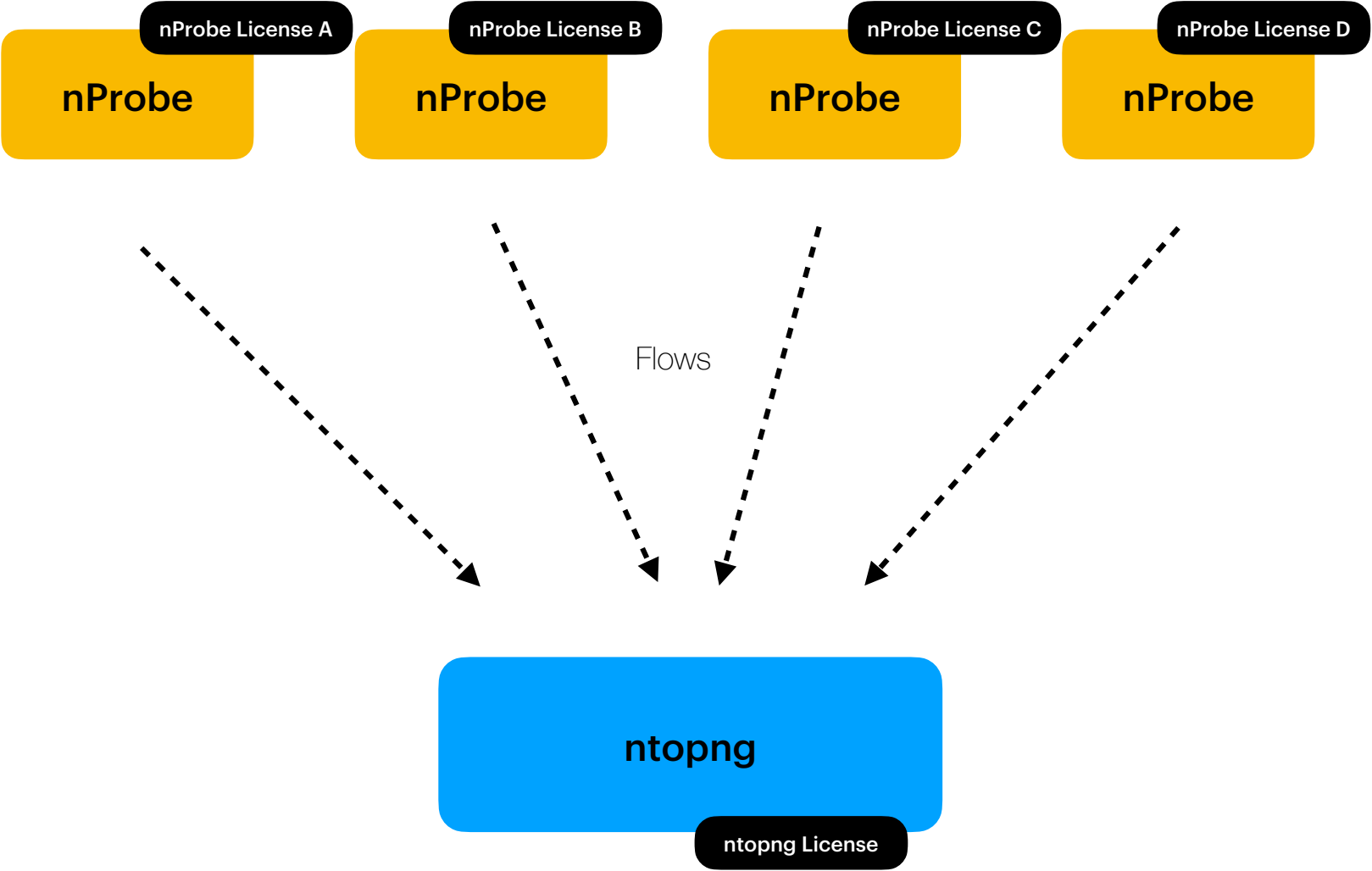
Remote Traffic Analysis



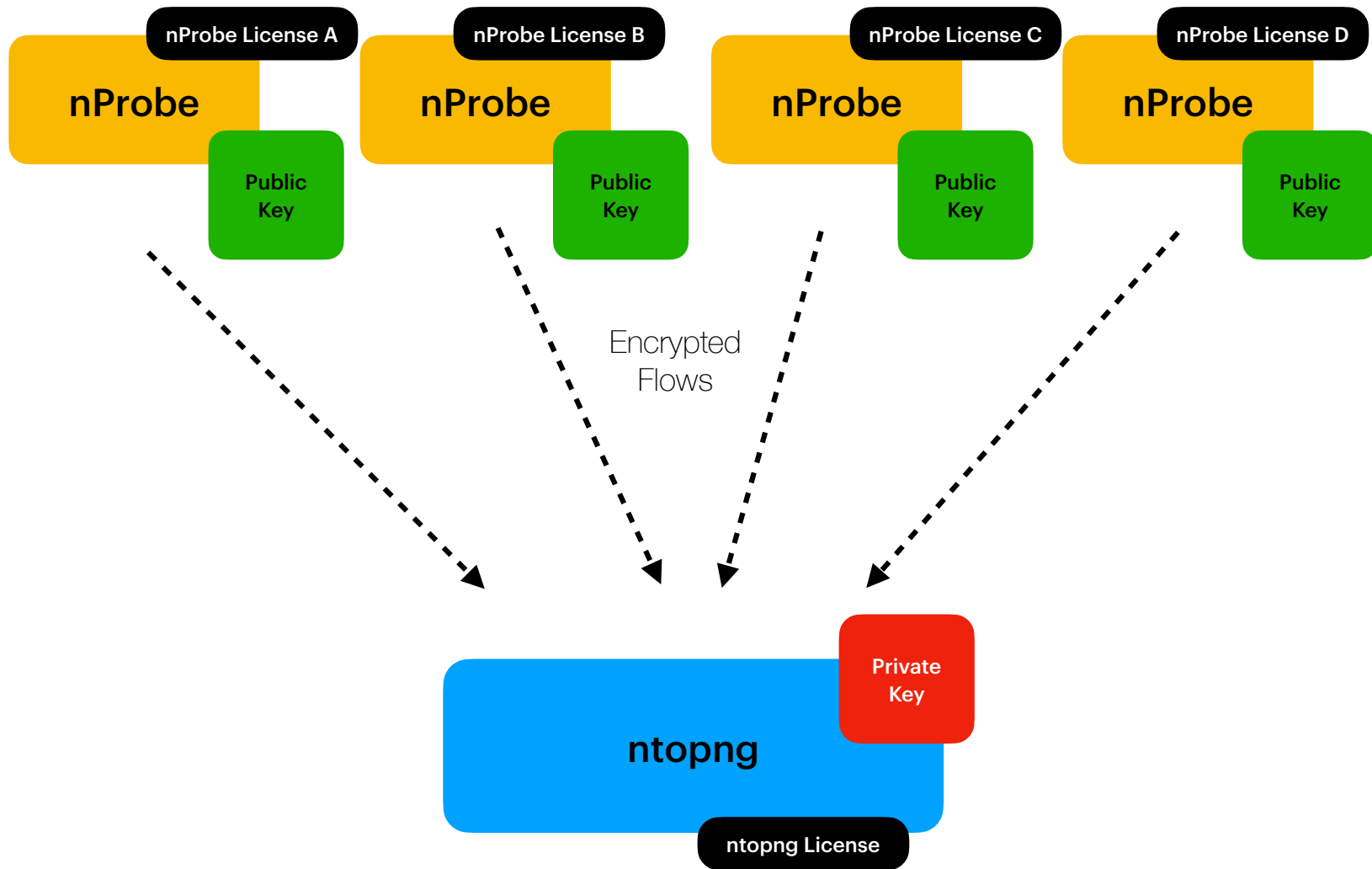
Remote Traffic Analysis



With Many Probes

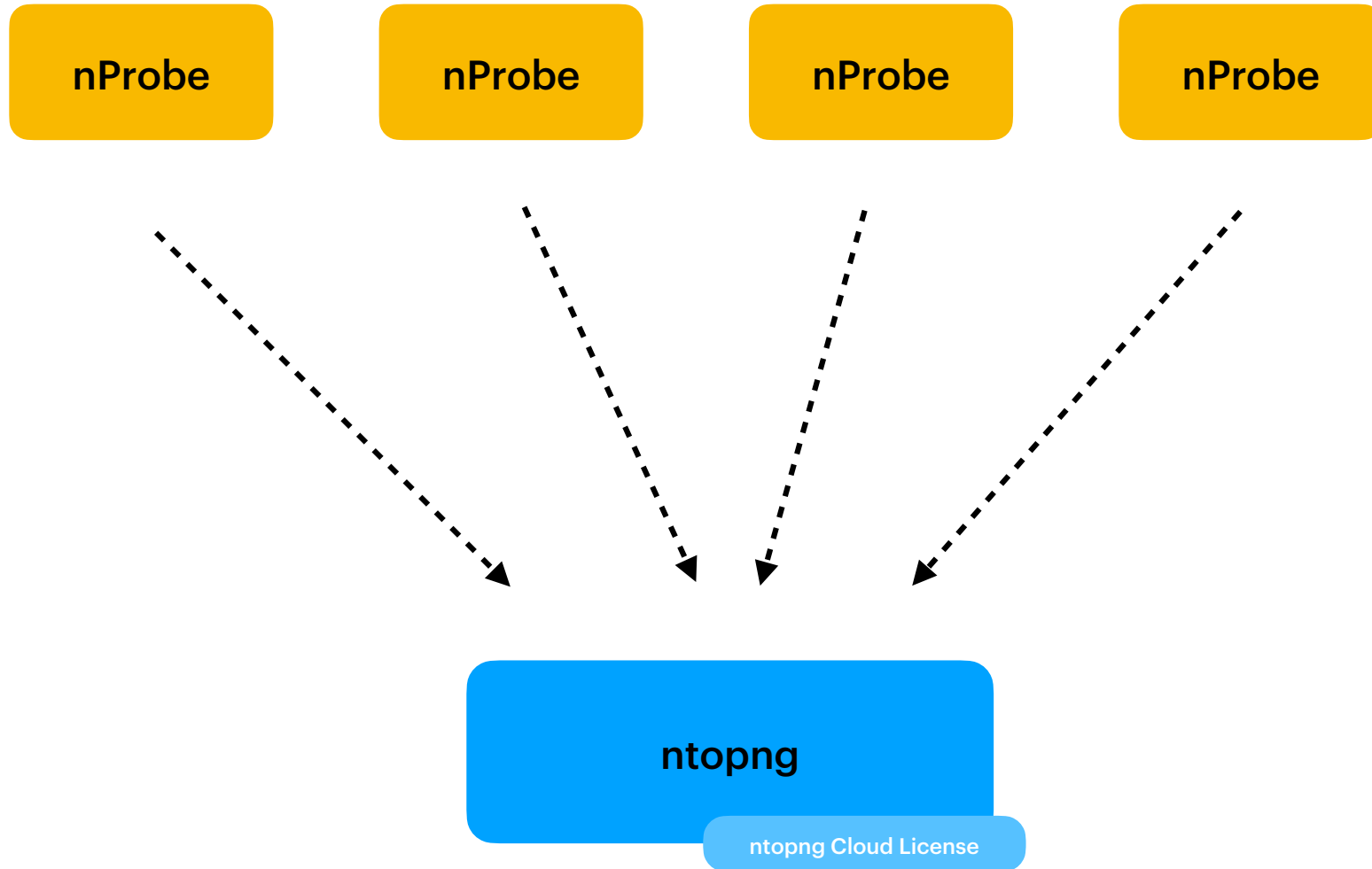


With (Optional) Encryption



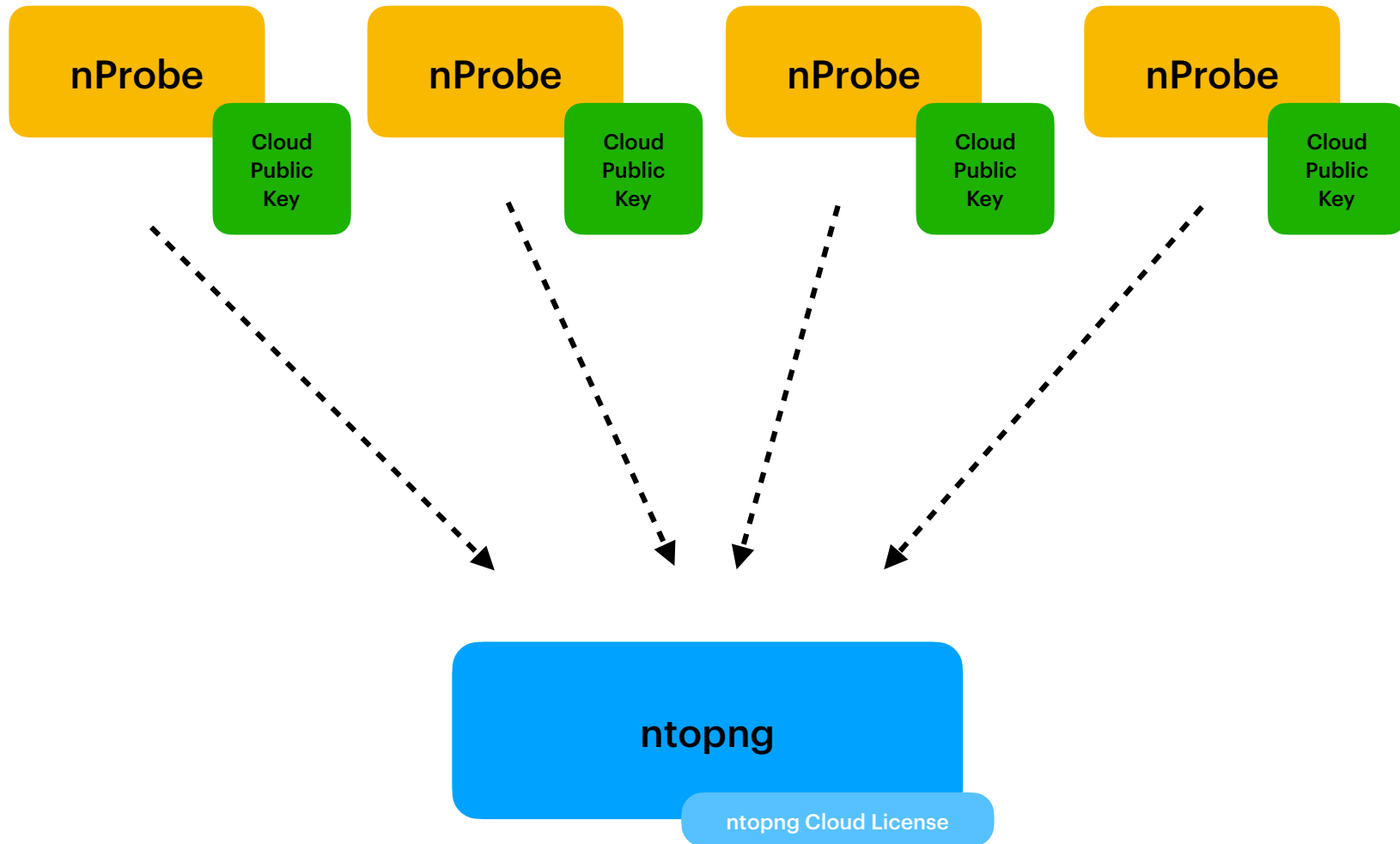
Cloud License

No per-probe license key required



Cloud License

Secure (Encrypted Export) by design



Bundle vs Cloud License

- Bundle
 - single key unlocking ntopng, nProbe, n2disk (they must run on the same box)
- Cloud
 - automatically unlocks remote nProbe instances
 - Designed for Service Providers
 - License the on-Cloud box and forget about System IDs on the probe side (just distribute the public key)
 - Anyone interested in early adoption? Contact us!



NTOPCONF '23

**SEPTEMBER 21
(TRAINING)-22
(CONFERENCE),
2023**



Submission Deadline

**JUNE 30TH,
2023**