ntopConf'23

What's new in the ntop suite

Alfredo Cardigliano <cardigliano@ntop.org>

ntopConf'23

Sept, 21-22 · Pisa

In This Presentation

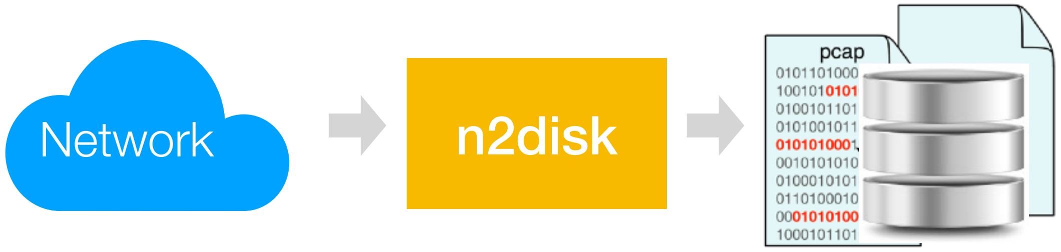
- n2disk: Smart Traffic Recording
- PF_RING: Latest Release and New Features
- nBox UI: The Brand New UI for ntop Appliances

n2disk

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 then the rest of the traffic

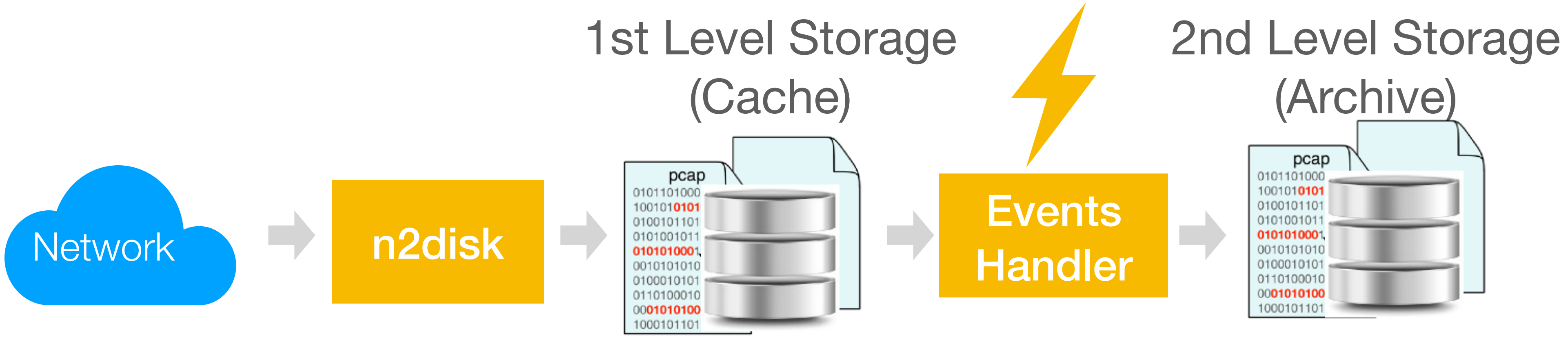
- What we need is:

  - Prioritize selected traffic (e.g. security alerts)

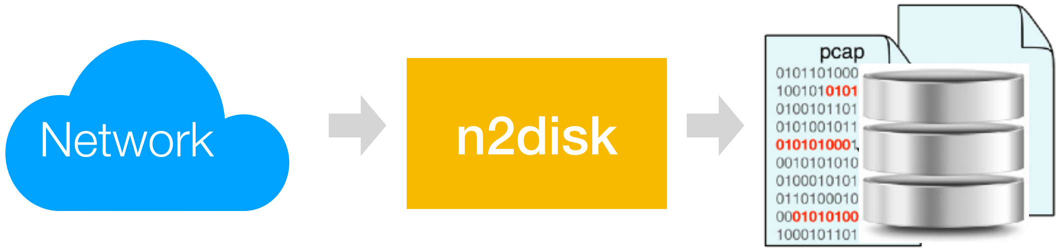
  - Smart data recycling: delete traffic which is not matching any event first

Smart Data Retention

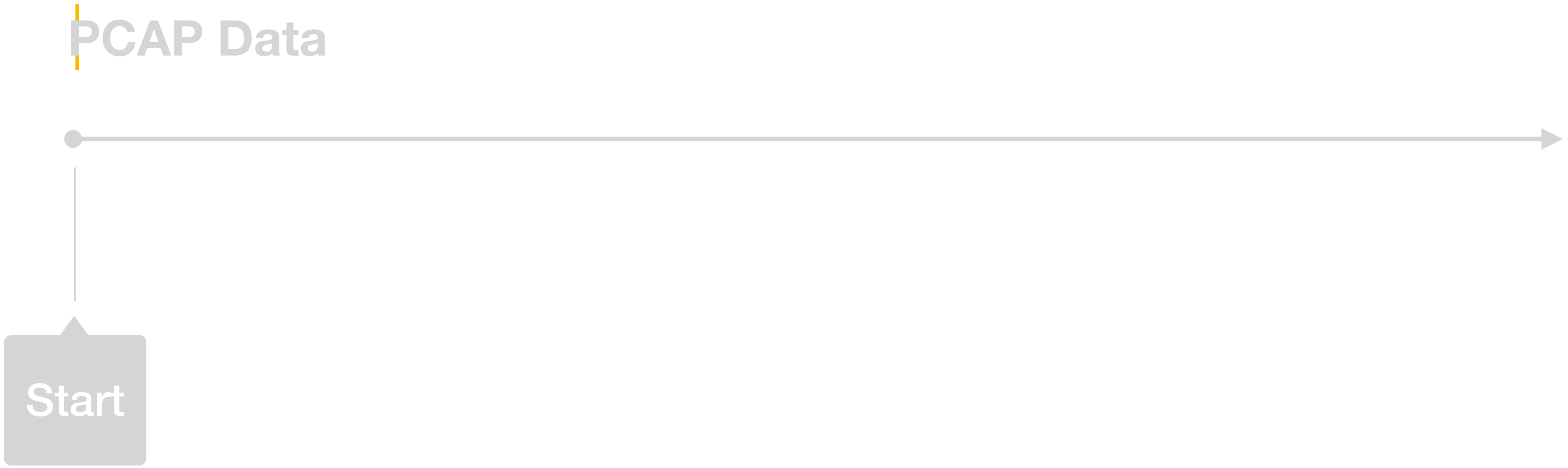
- Process Network events generated by ntopng
- Use a 1st level storage to implement continuous recording with a short data retention (cache)
- Use a 2nd level storage to archive traffic for Network events with a longer data retention (archive)



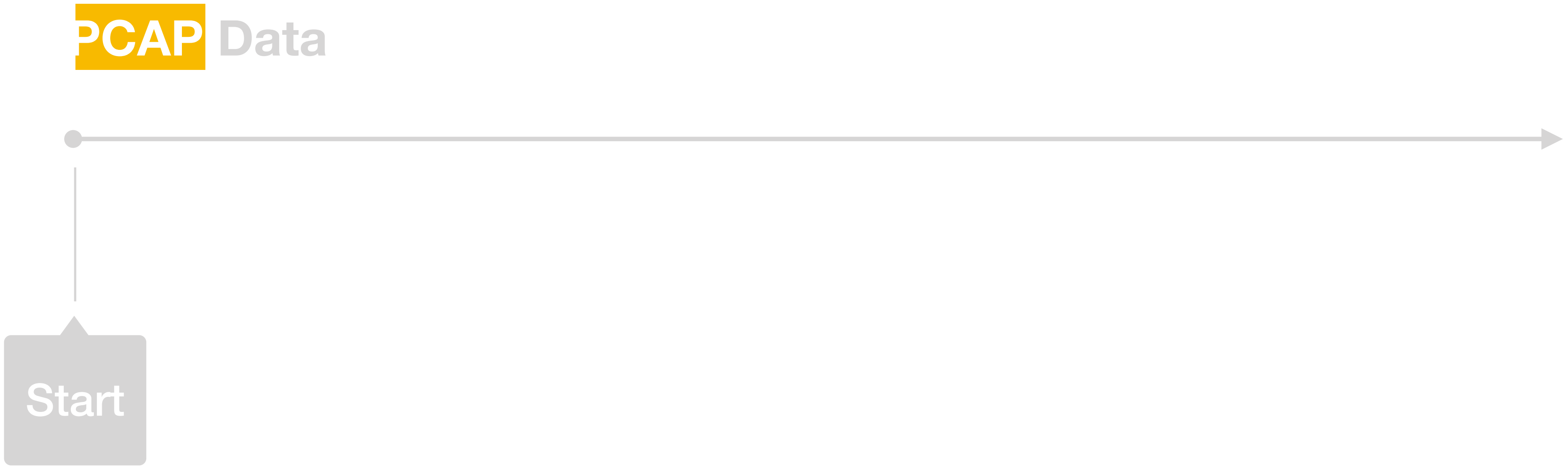
Continuous Recording



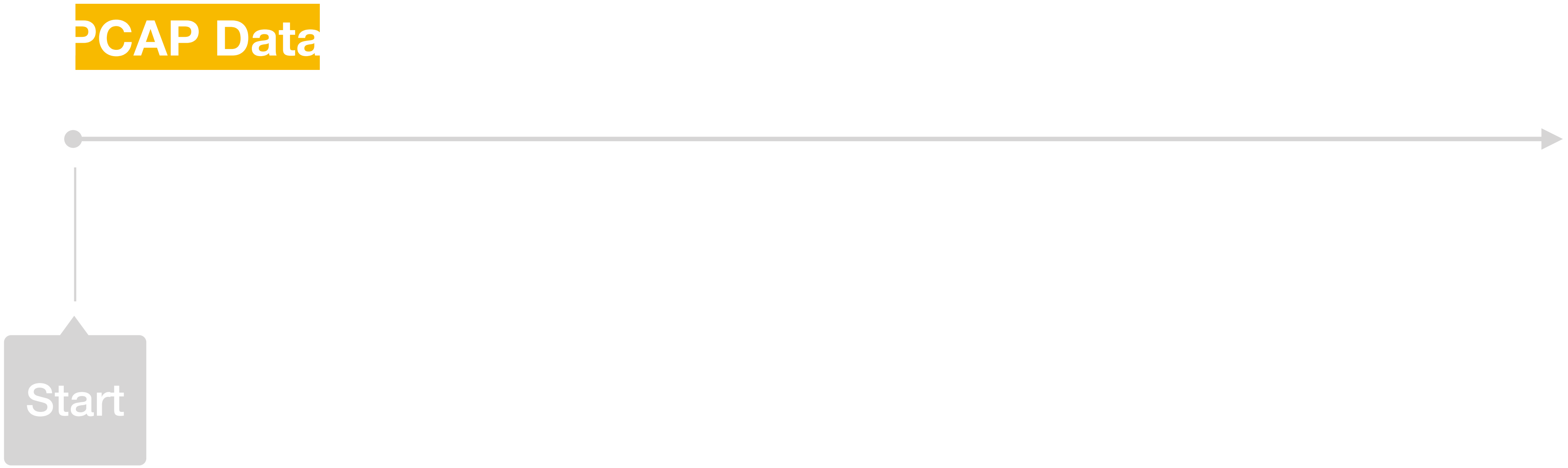
Continuous Recording



Continuous Recording



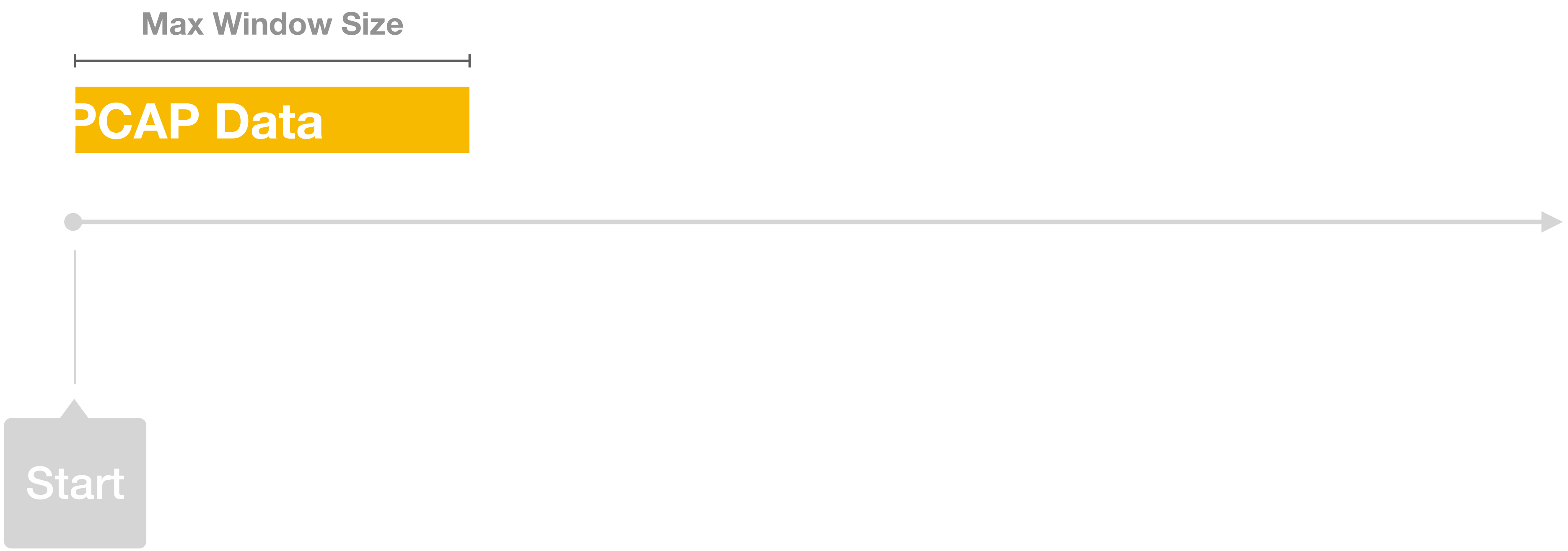
Continuous Recording



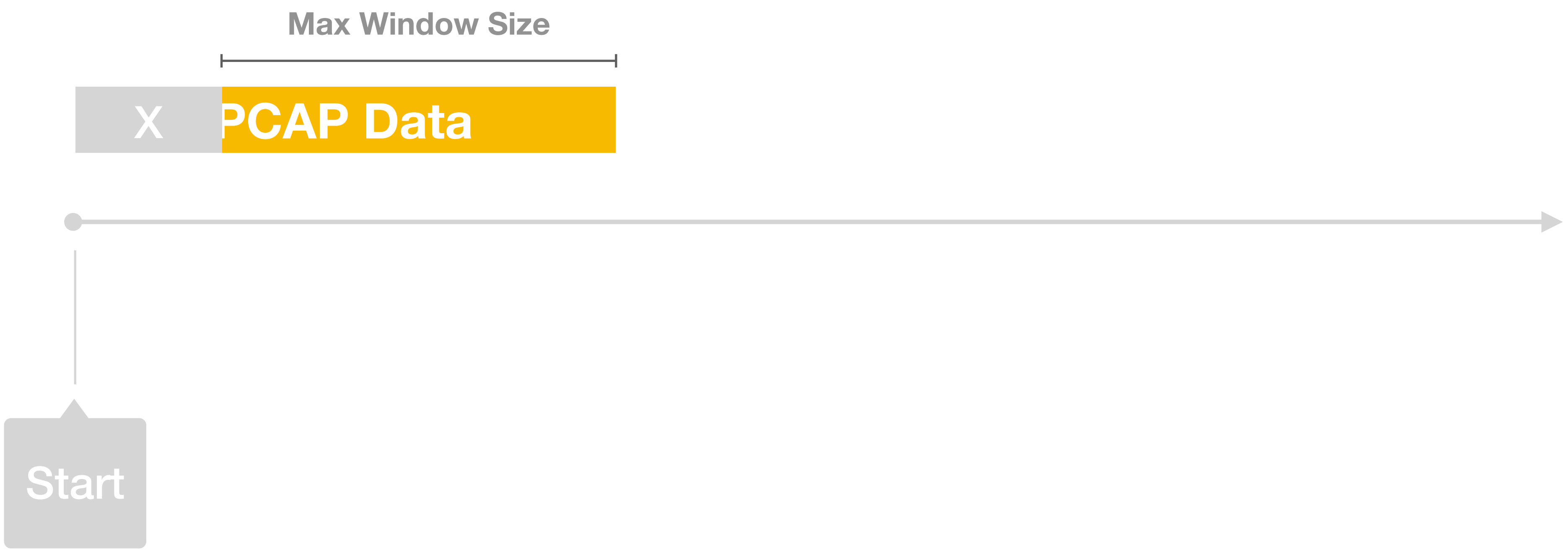
PCAP Data

Start

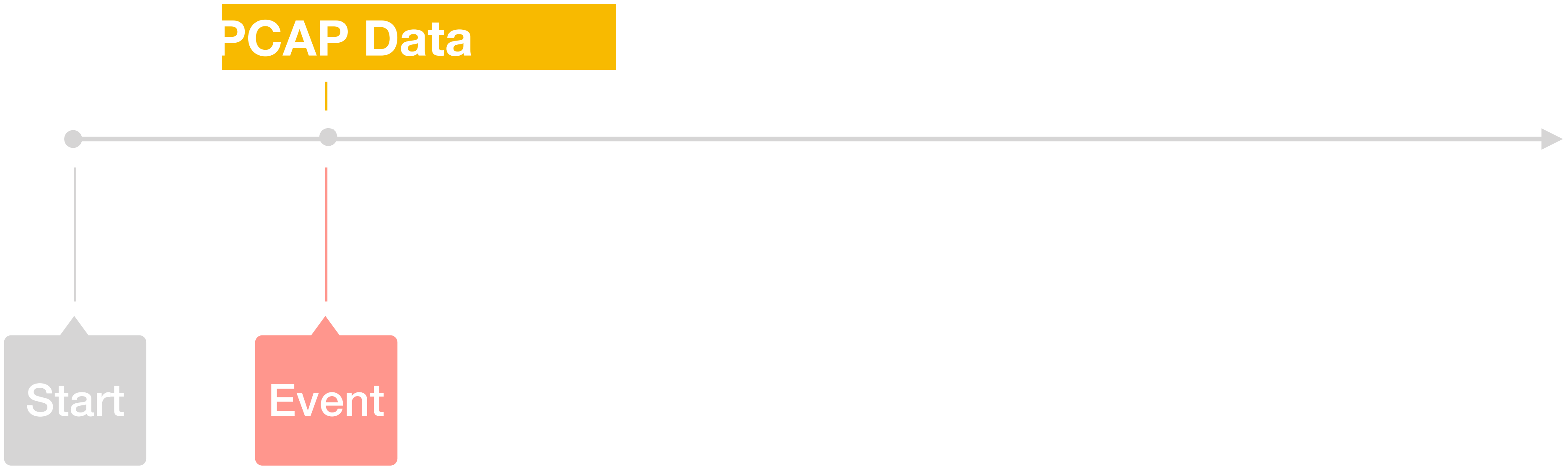
Continuous Recording



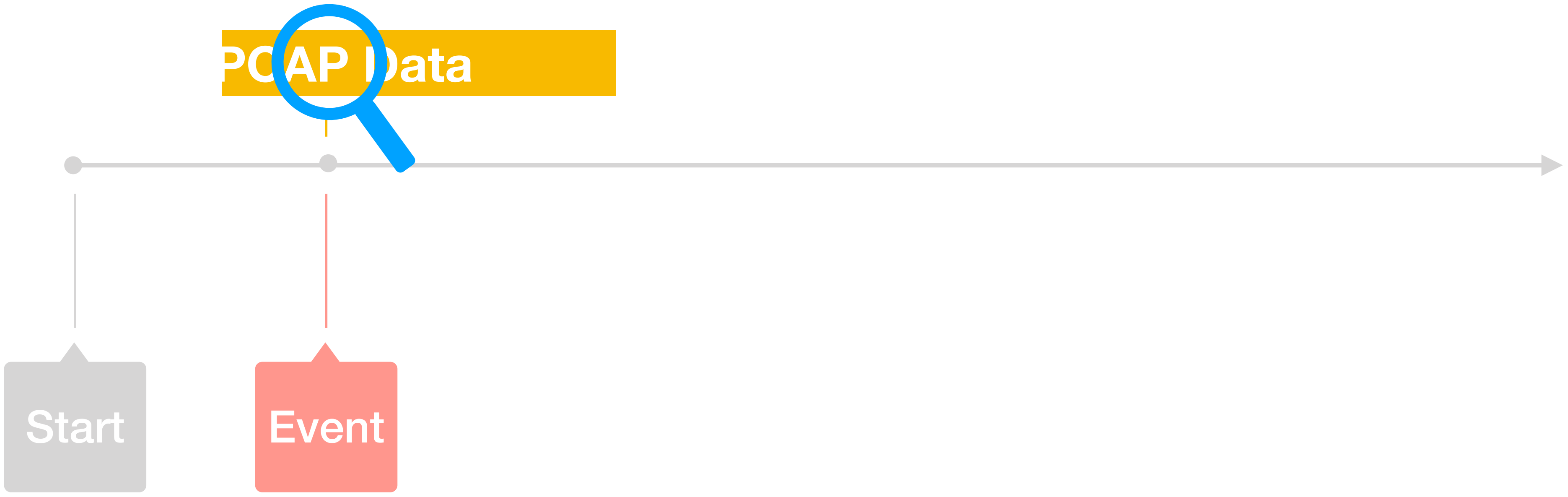
Continuous Recording



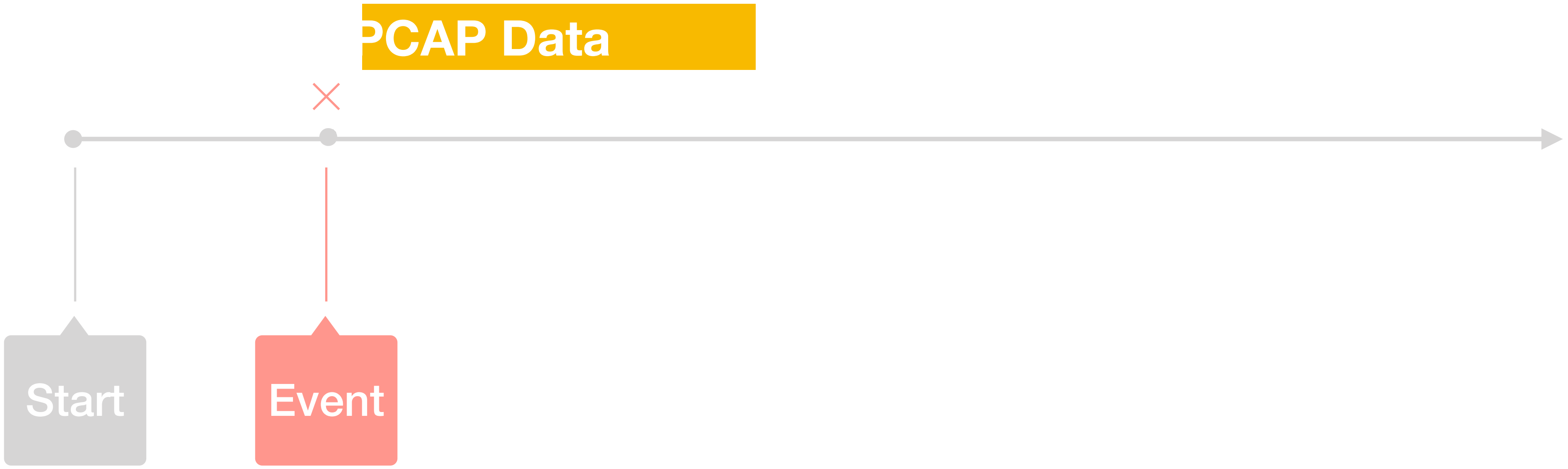
Continuous Recording



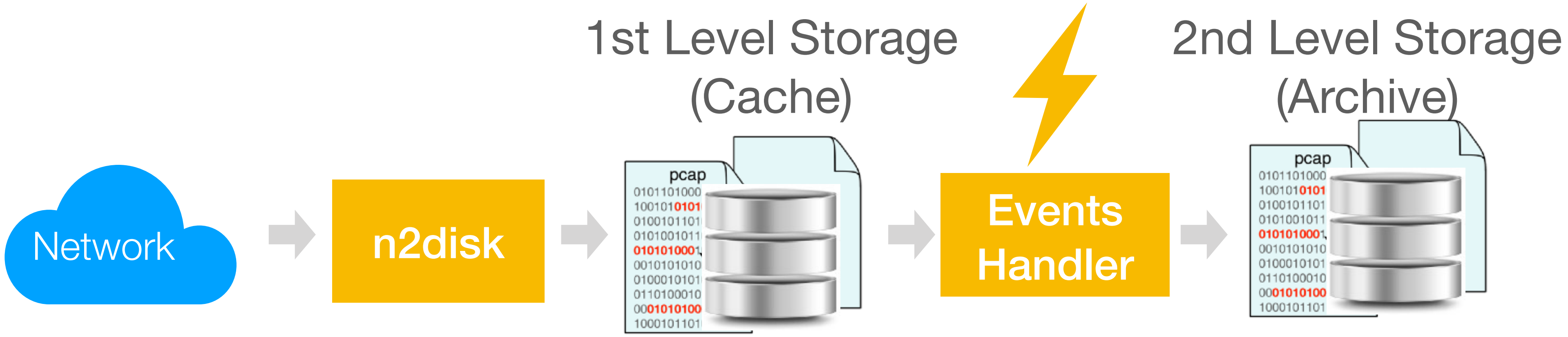
Continuous Recording



Continuous Recording



Smart Recording



Network

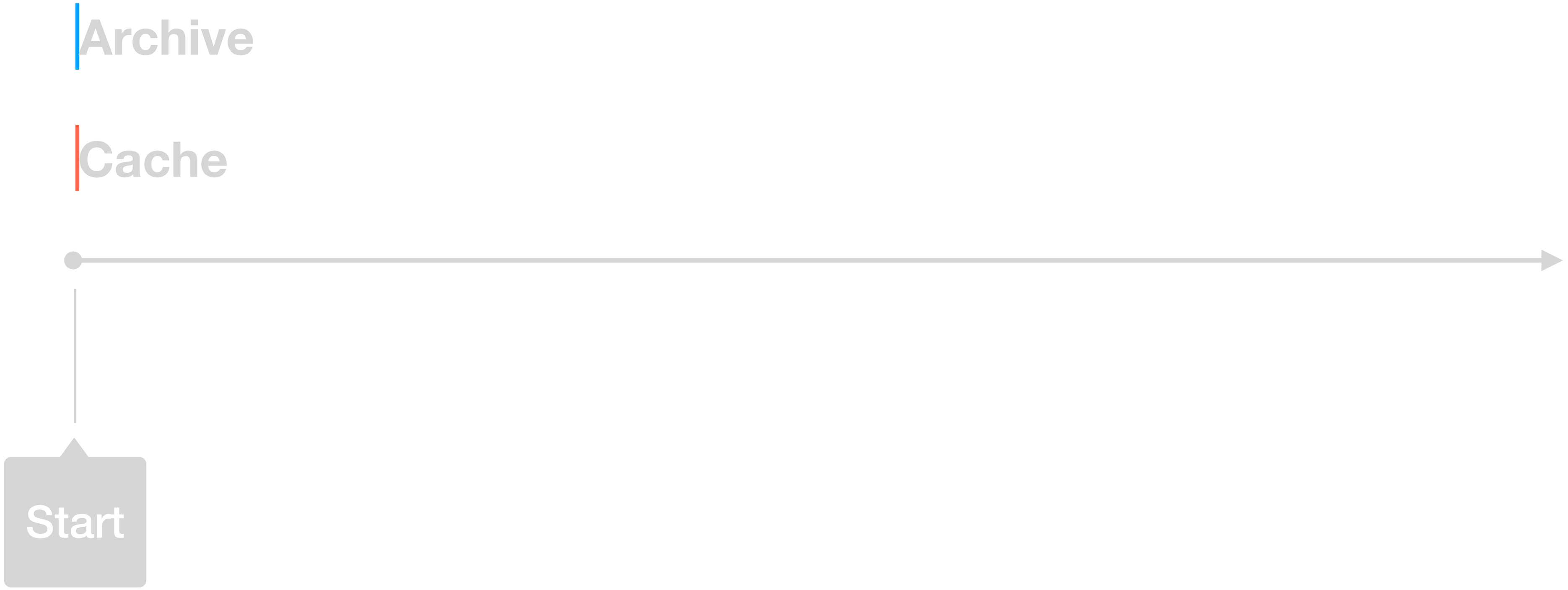
n2disk

1st Level Storage (Cache)

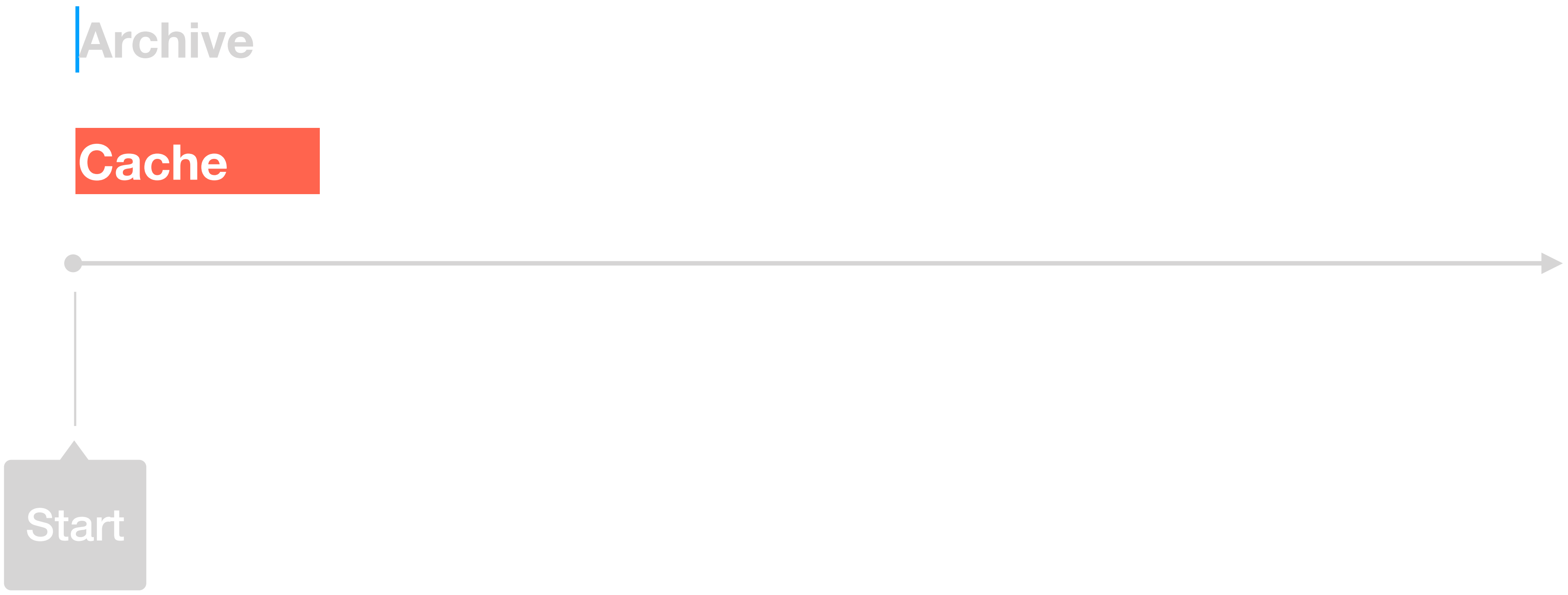
Events Handler

2nd Level Storage (Archive)

Smart Recording



Smart Recording

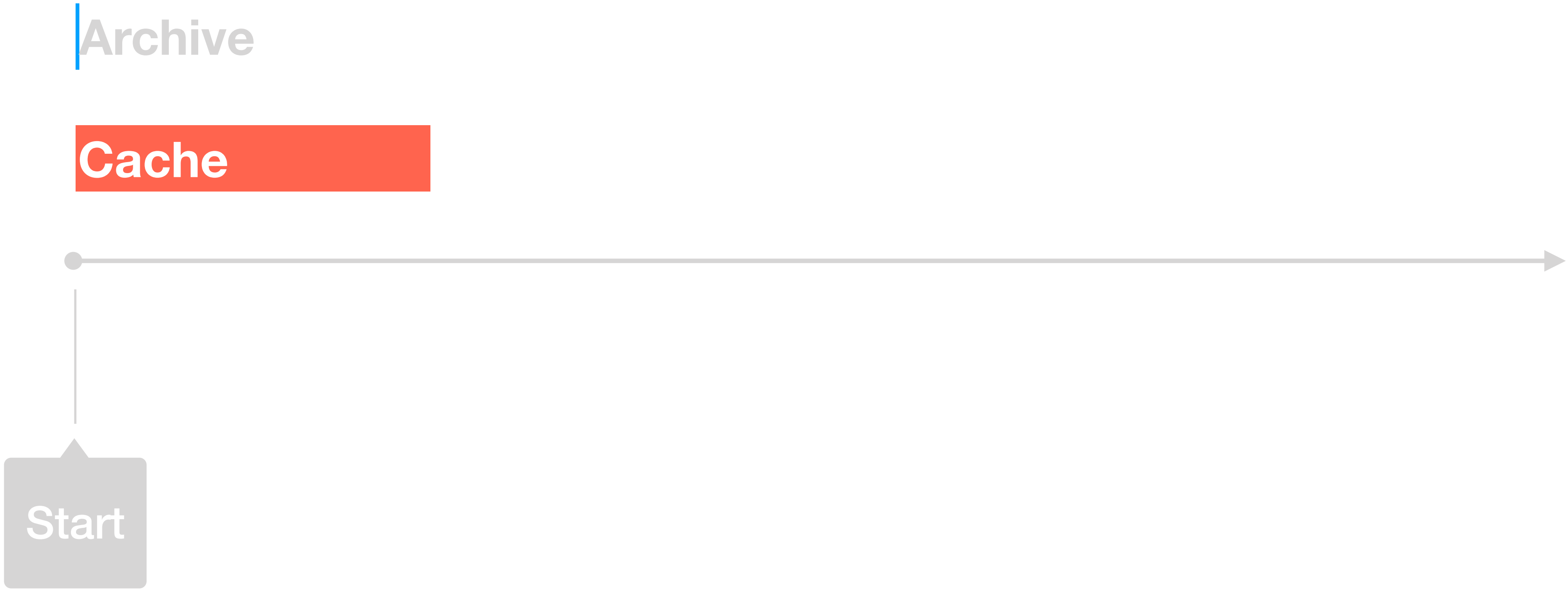


Archive

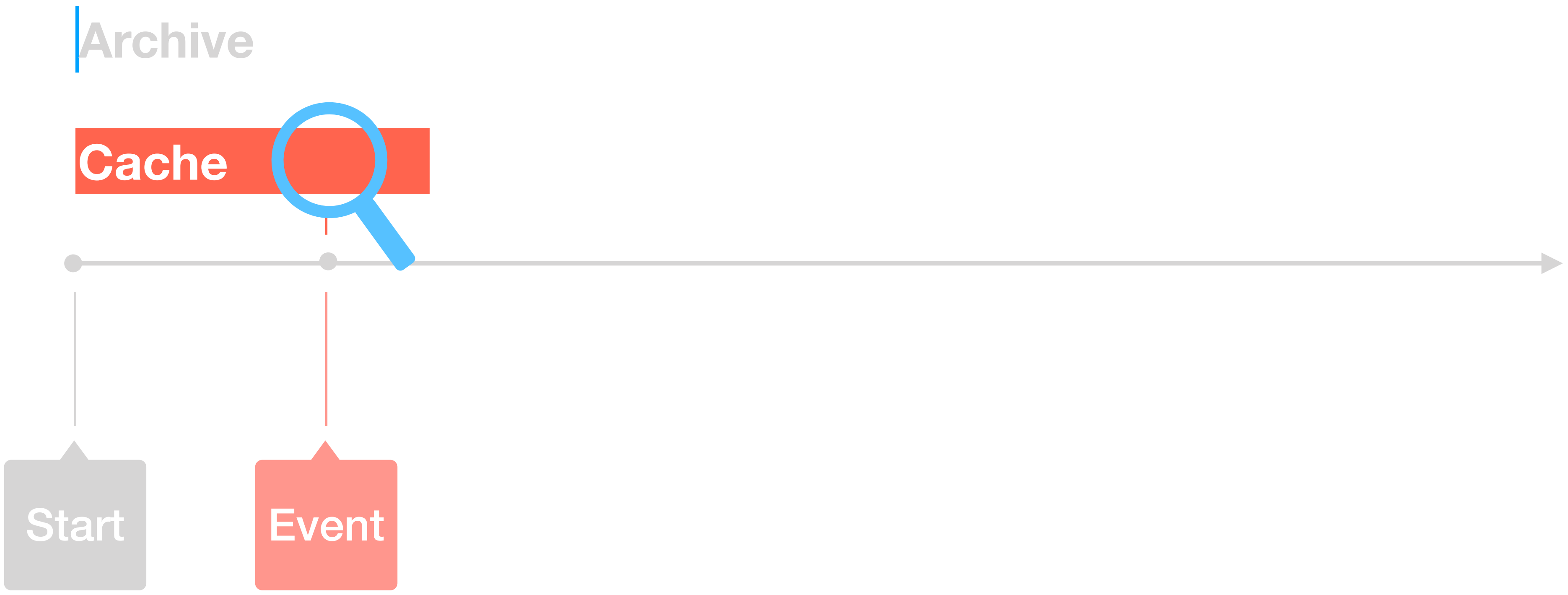
Cache

Start

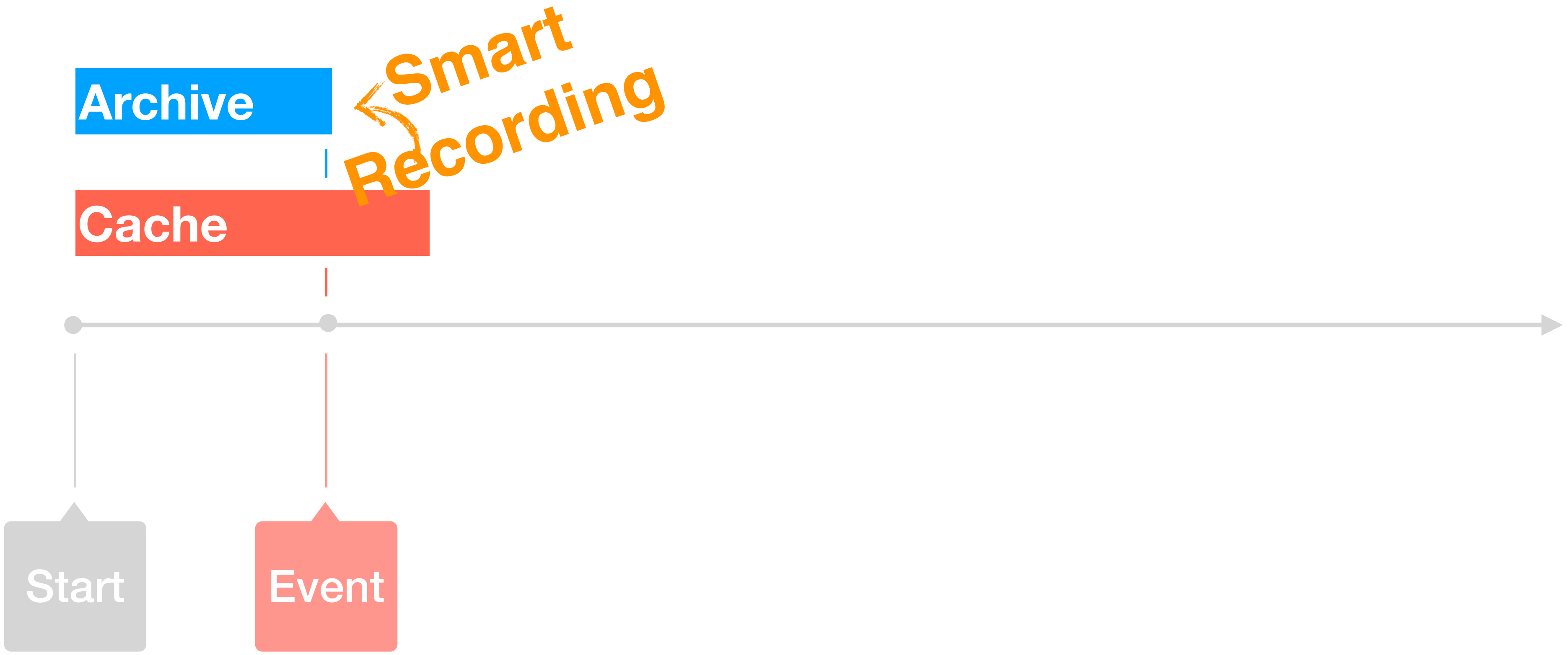
Smart Recording



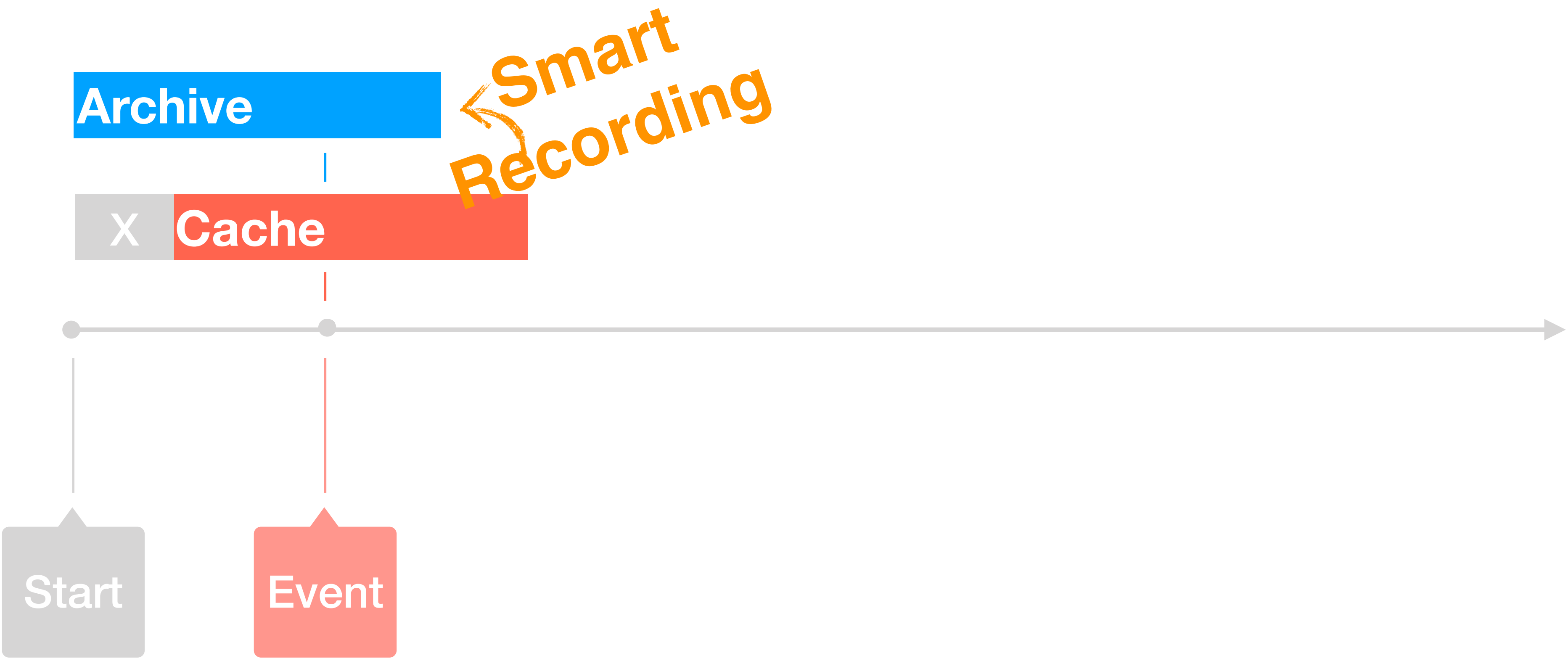
Smart Recording



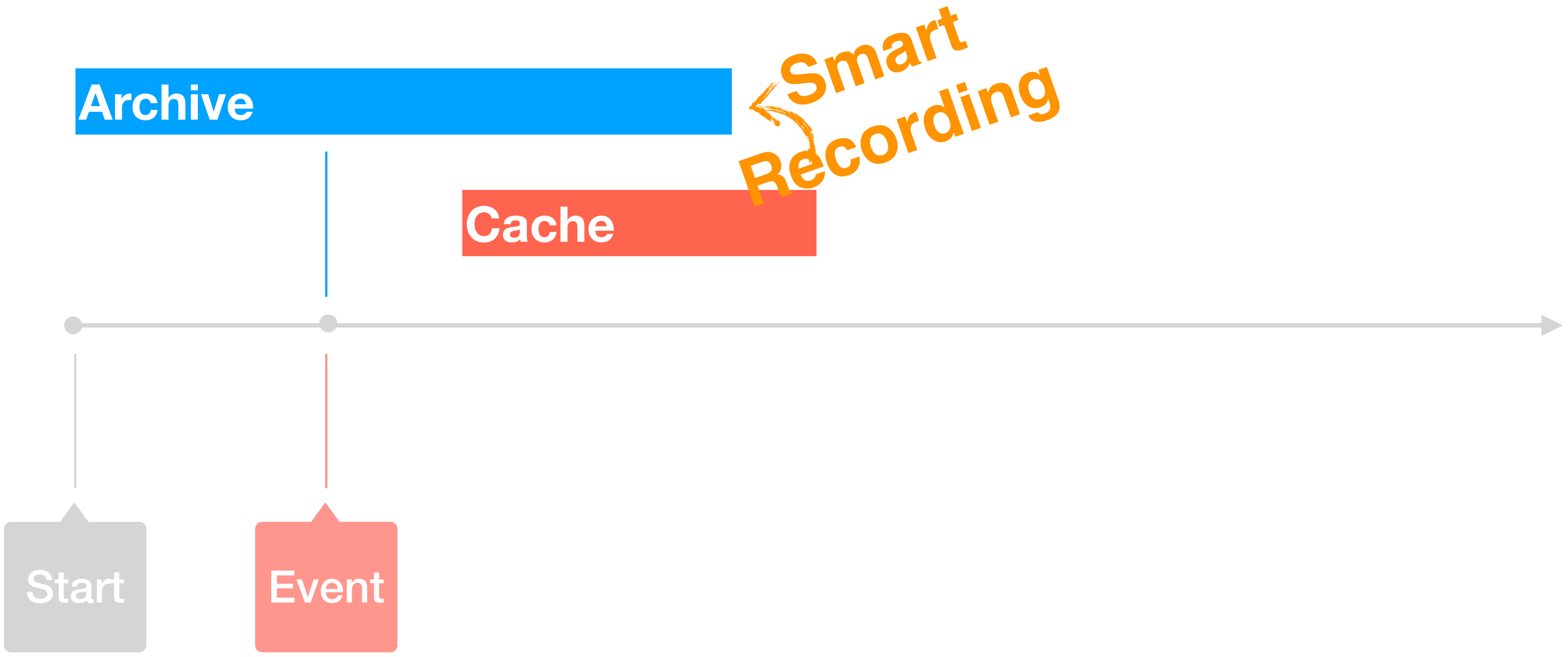
Smart Recording



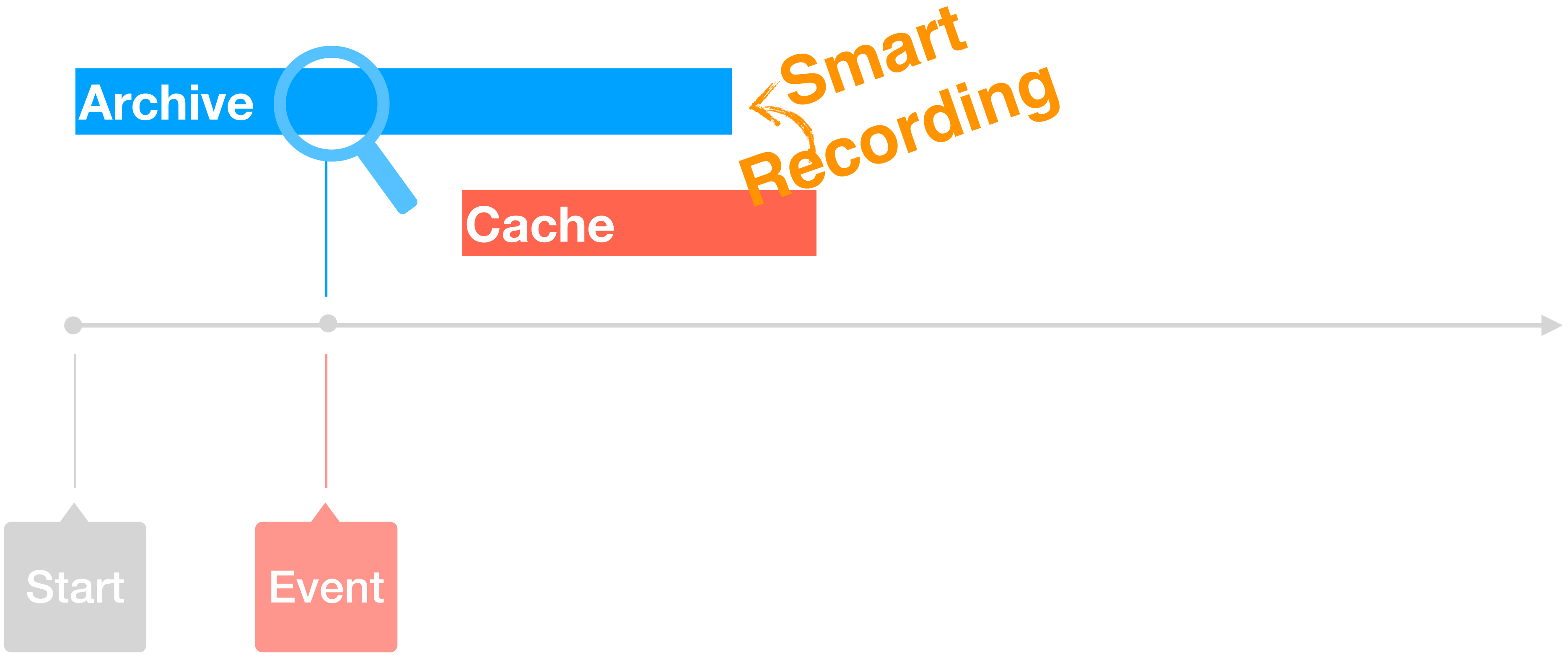
Smart Recording



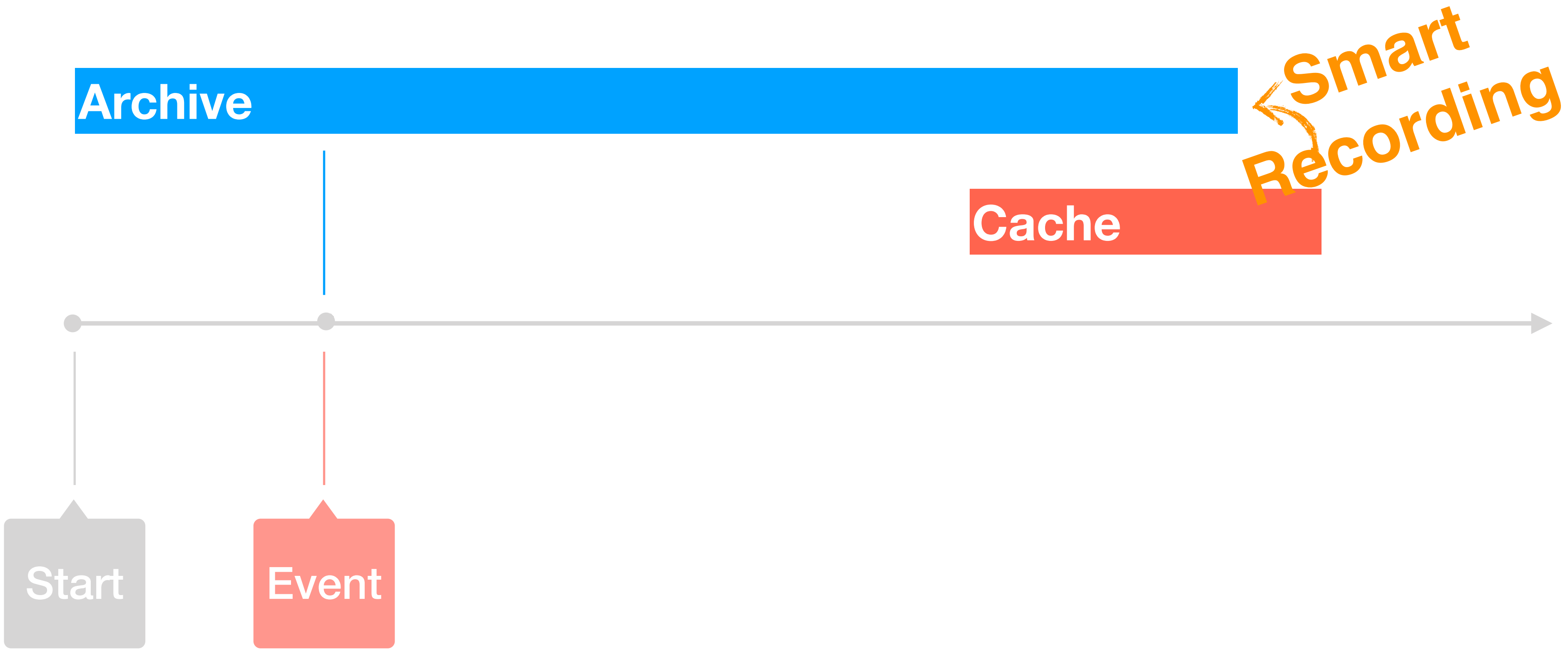
Smart Recording



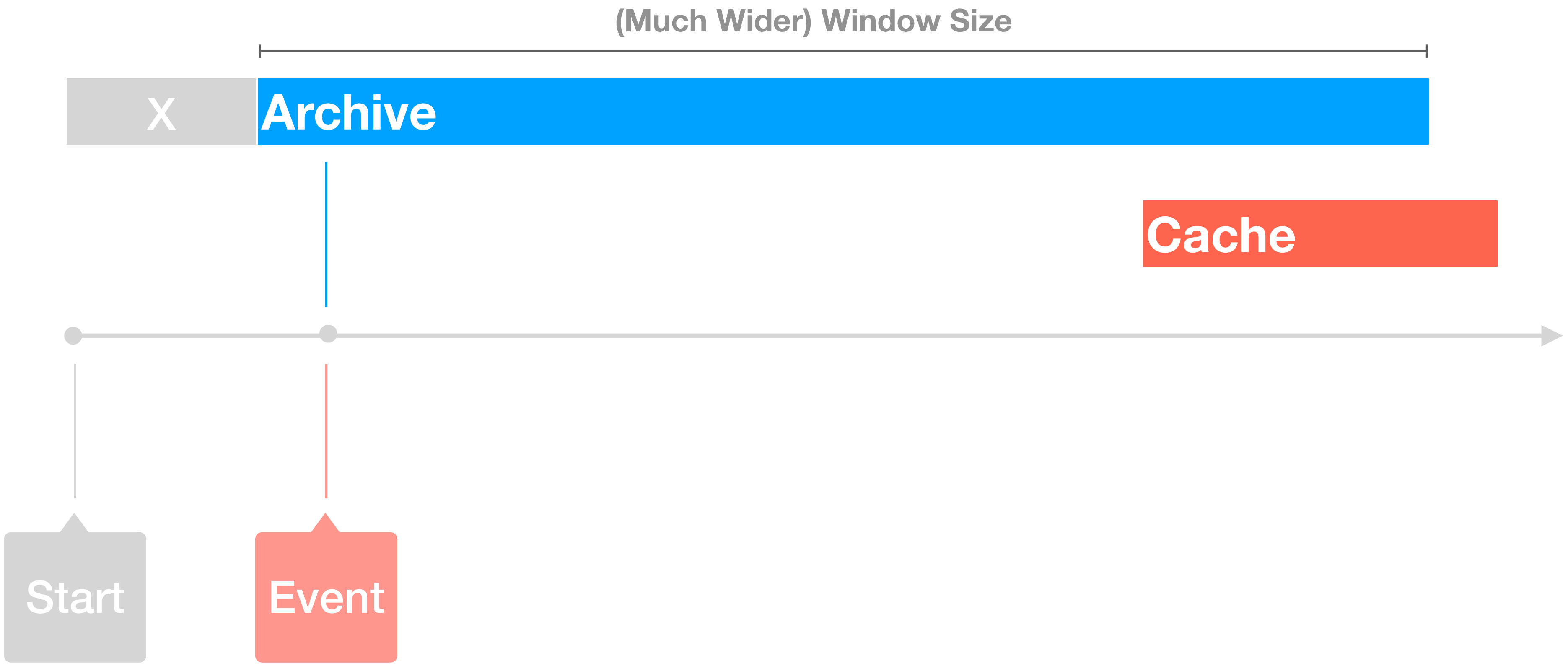
Smart Recording



Smart Recording



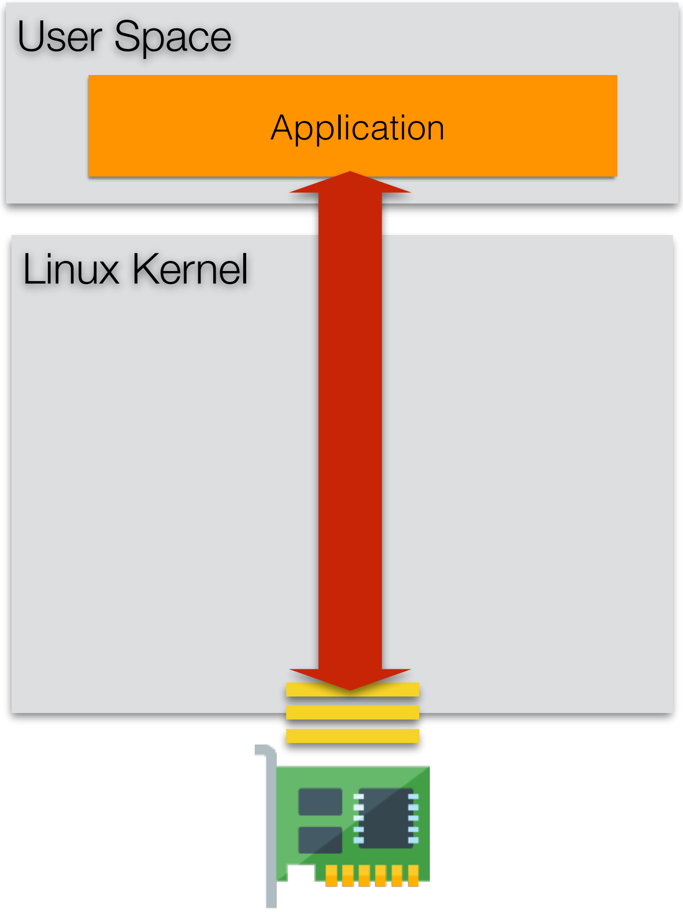
Smart Recording



PF_RING

Quick Recap

- As of today PF_RING provides:
  - Packet capture acceleration with any adapter using Linux kernel drivers (limited boost)
  - XDP (Linux eXpress Data Path) acceleration with Linux drivers supporting AF_XDP
  - Best acceleration (Zero-Copy Kernel-Bypass) with PF_RING ZC drivers up to 100 Gbps with:
    - Commodity adapters from Intel, NVIDIA / Mellanox
    - FPGA adapters from Napatech, Silicom FPGA and other vendors



PF_RING 8.6

- Just released (Sept 2023)
- New Runtime component
  - Push filtering rules on the fly at runtime
- New driver for NVIDIA/Mellanox ConnectX
- New driver for Intel VFs
- Support for Debian 12 and latest 6.x kernels

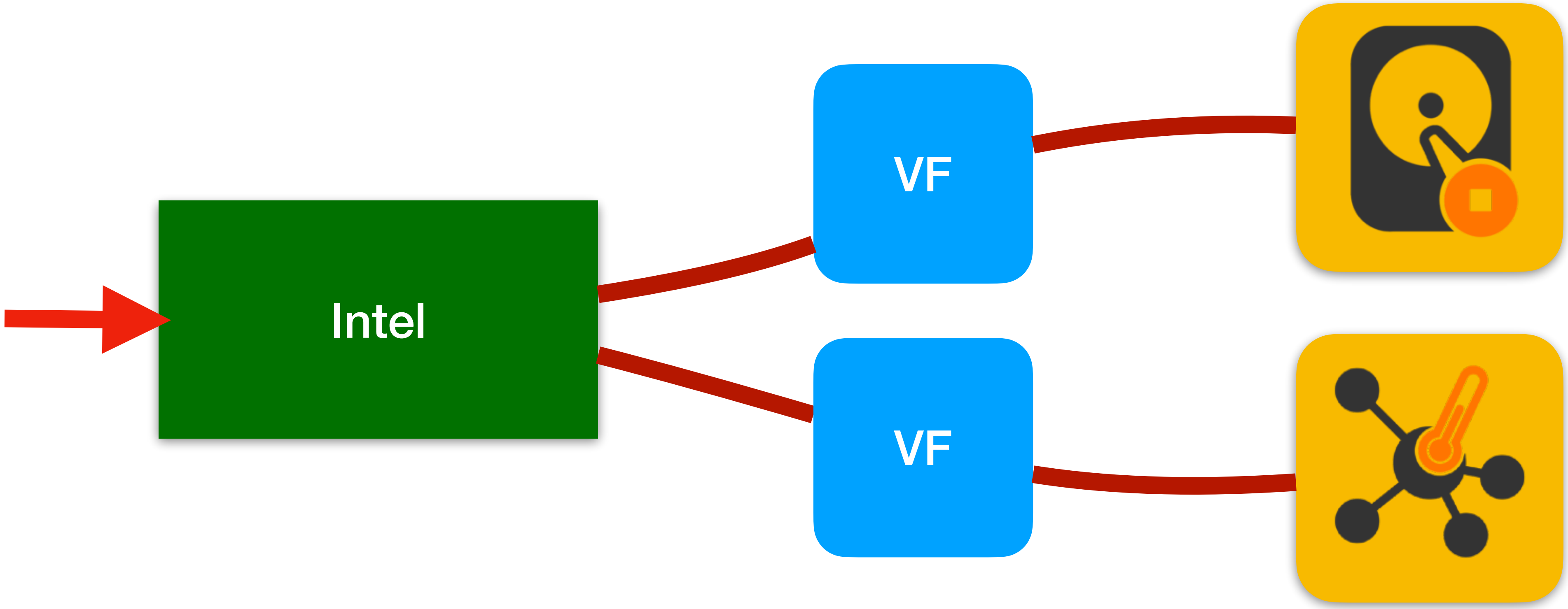
Intel Adapters

- Supported families:
  - **e1000e** (8254x/8256x/8257x/8258x)
  - **igb** (82575/82576/82580/I350)
  - **ixgbe** (82599/X520/X540/X550)
    - **ixgbevf** (ixgbe VF)
  - **i40e** (X710/XL710/XXV710)
    - **iavf** (i40e VF) NEW
  - **ice** (E810)
  - ~~**fm10k**~~

DEPRECATED

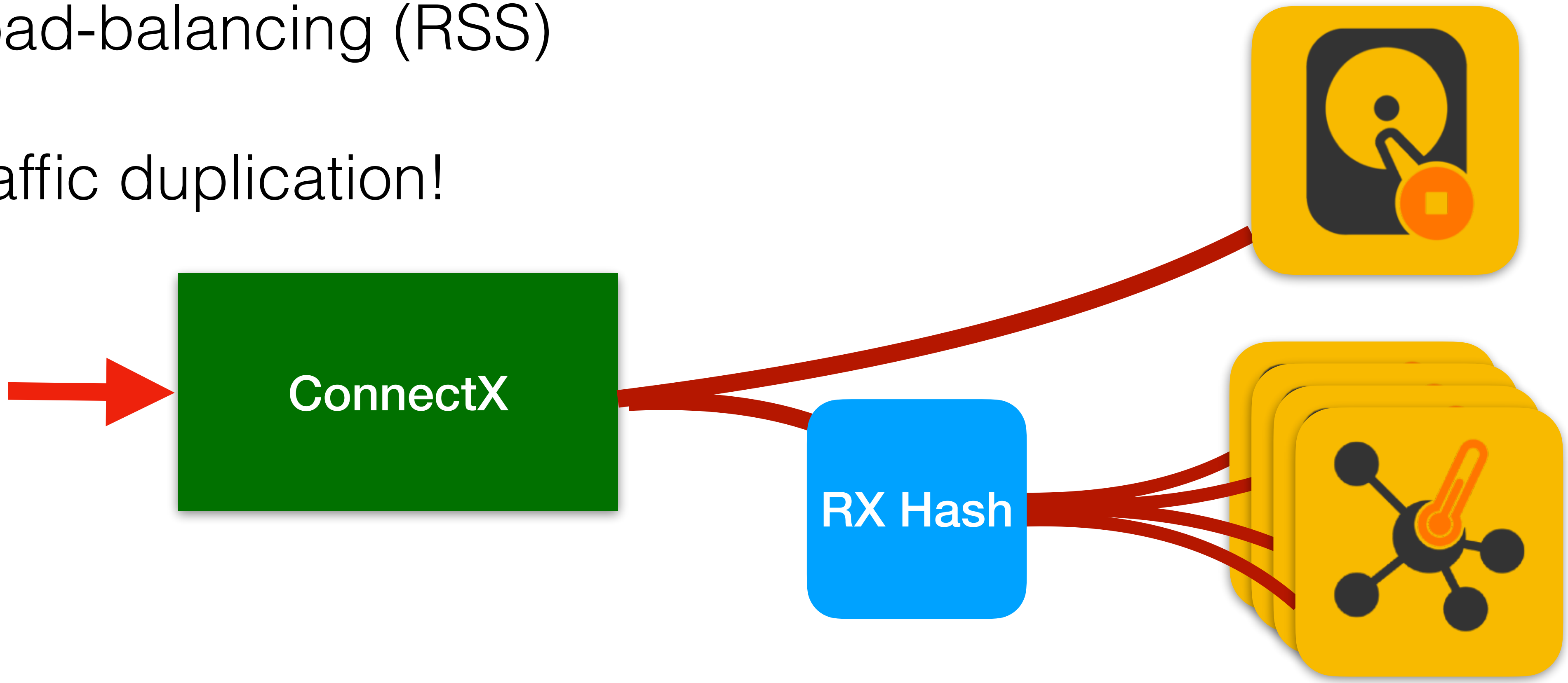
Intel with VFs

- SR-IOV Virtual Functions are virtualized instances of the physical interface (usually used by VMs)
- Traffic is steered to VFs based on MAC (and VLAN)
- i40e VFs (iavf) support **trust mode** which enables promiscuous capture (with **duplication**!)

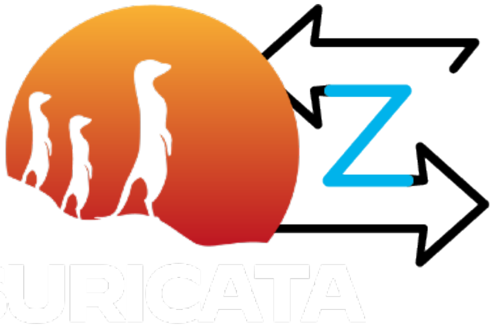


NVIDIA/Mellanox Adapters

- PF_RING ZC driver for ConnectX 4/5/6 NEW
- Performance up to 100 Gbps
- Hardware packet timestamps
- Hardware packet filtering
- Load-balancing (RSS)
- Traffic duplication!

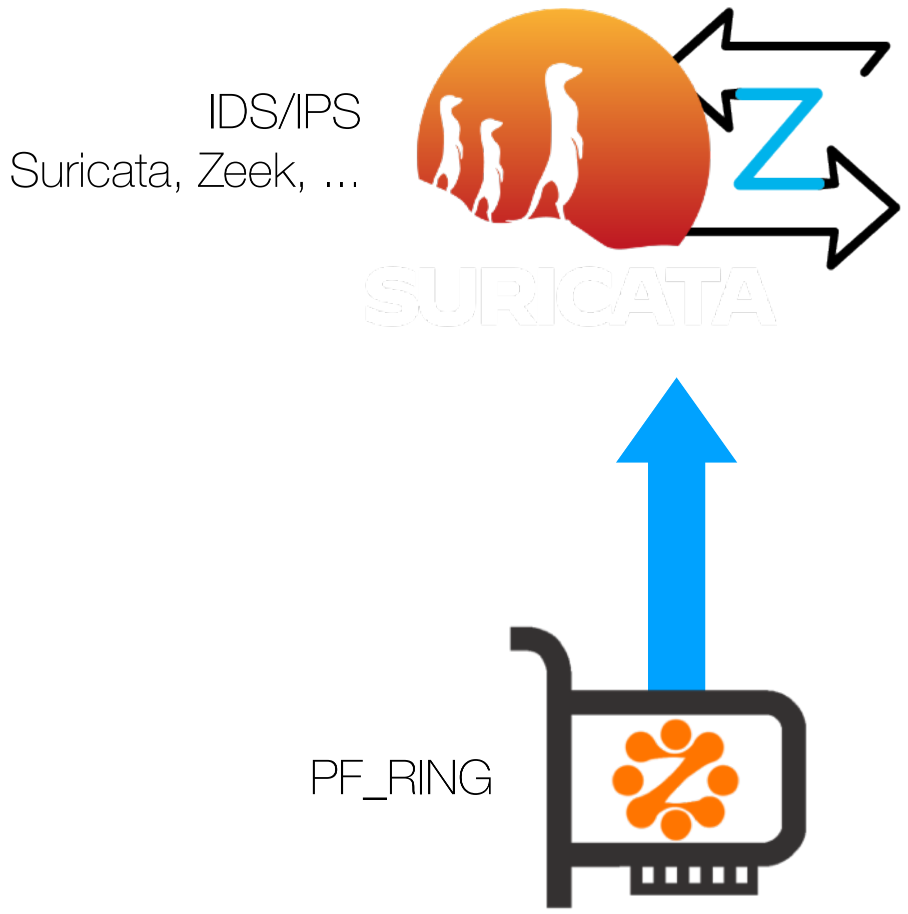


IDS Acceleration

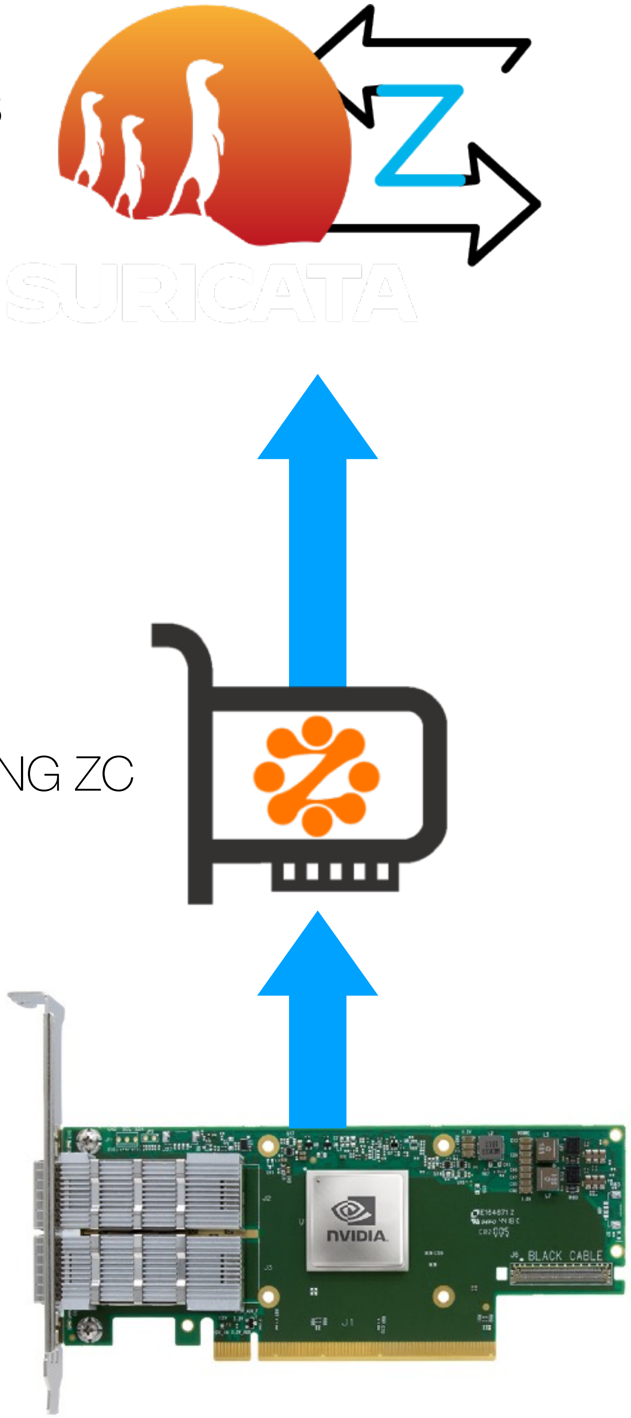


IDS/IPS
Suricata, Zeek, ...

IDS Acceleration



IDS Acceleration

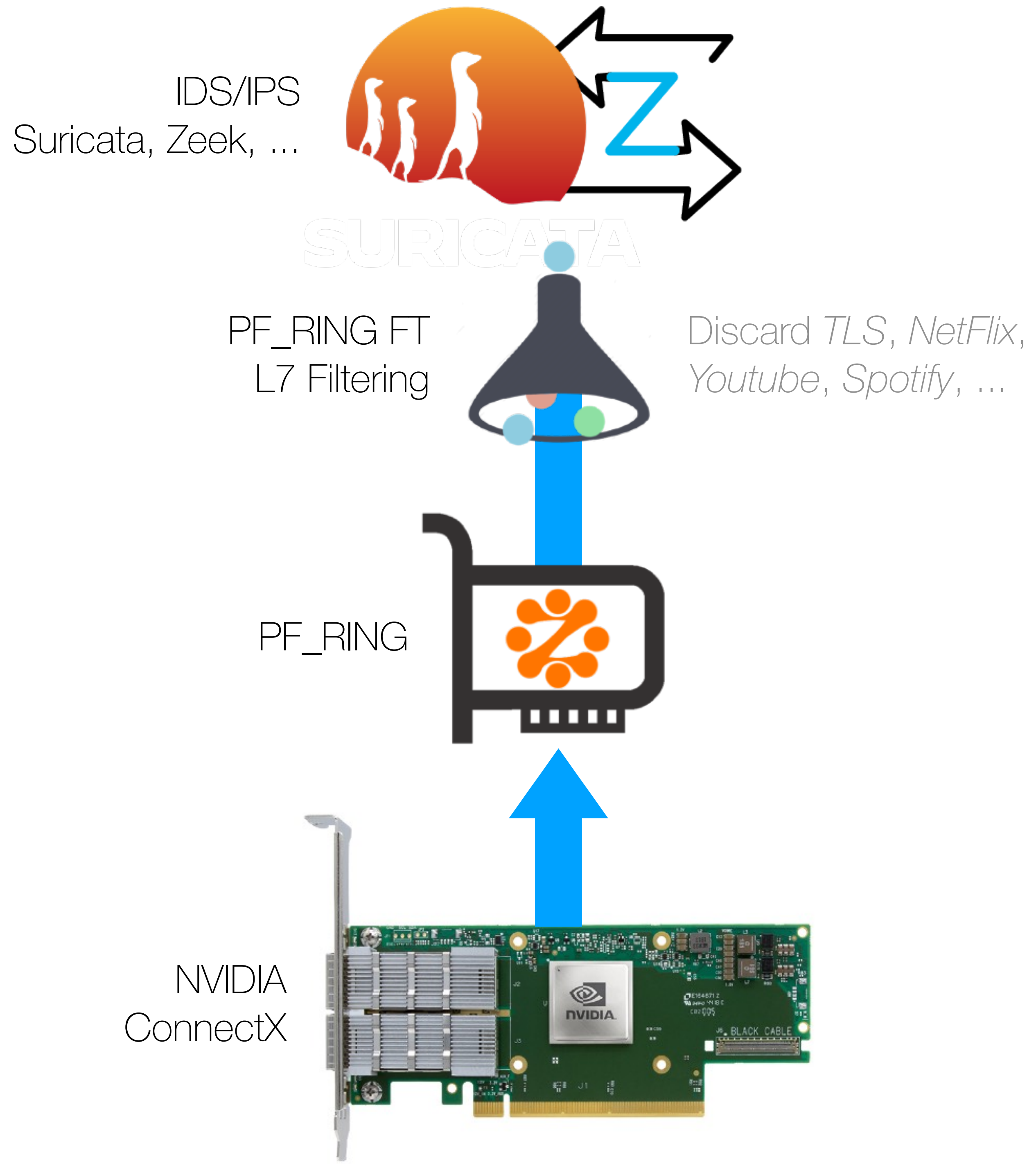


IDS/IPS
Suricata, Zeek, ...

PF_RING ZC

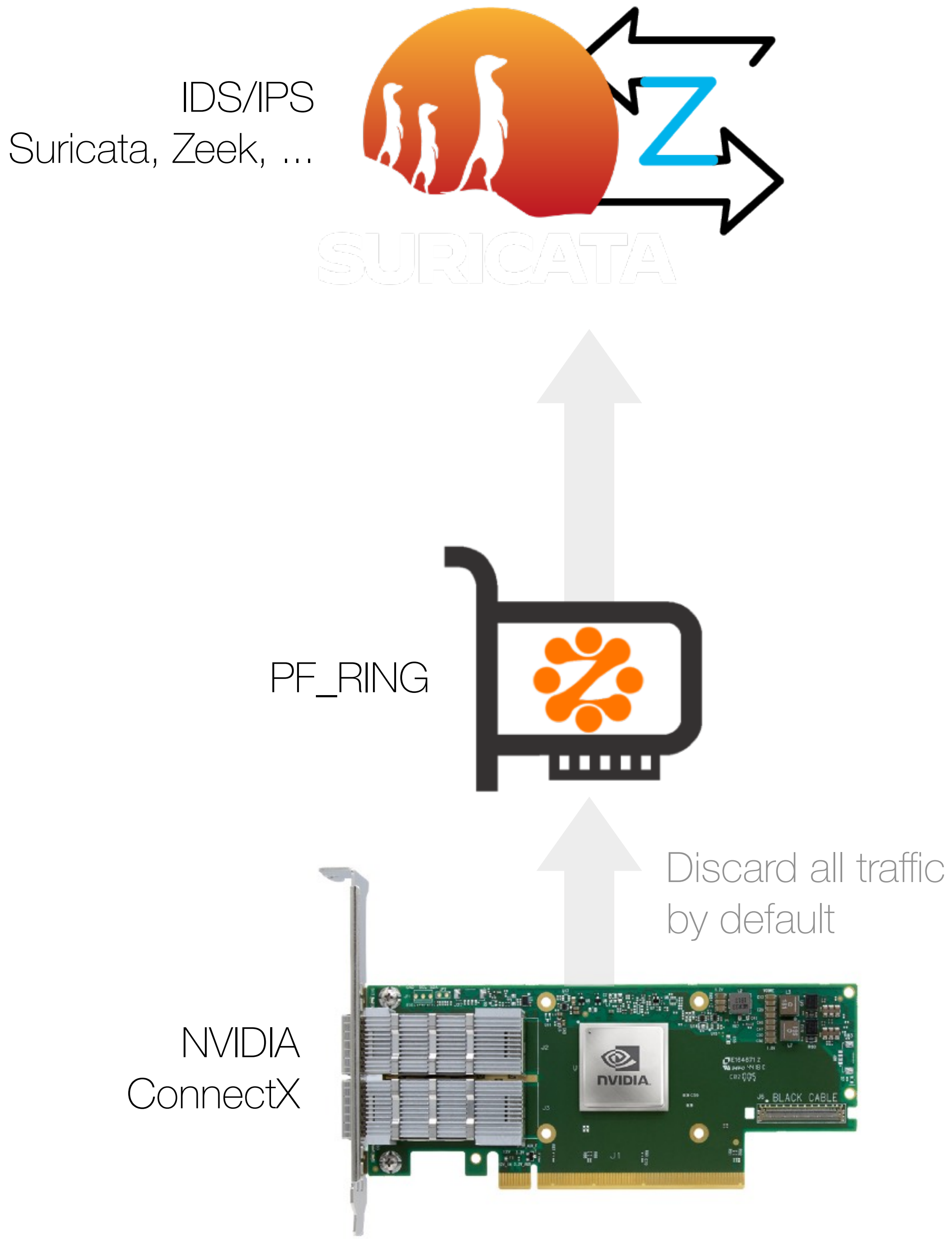
NVIDIA
ConnectX

IDS Acceleration



ntopConf'23

Suricata and Zeek On Demand



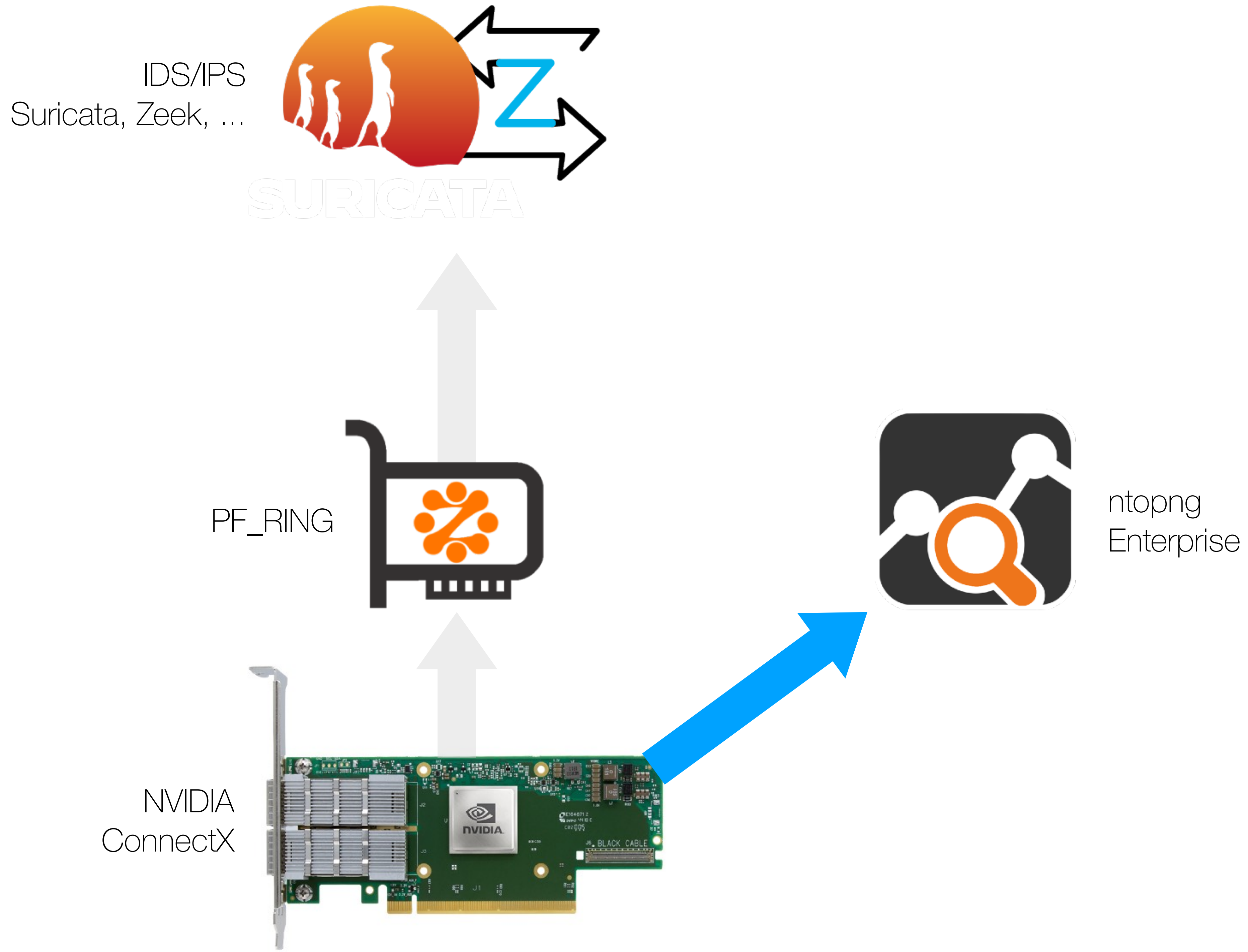
IDS/IPS
Suricata, Zeek, ...

PF_RING

Discard all traffic
by default

NVIDIA
ConnectX

Suricata and Zeek On Demand



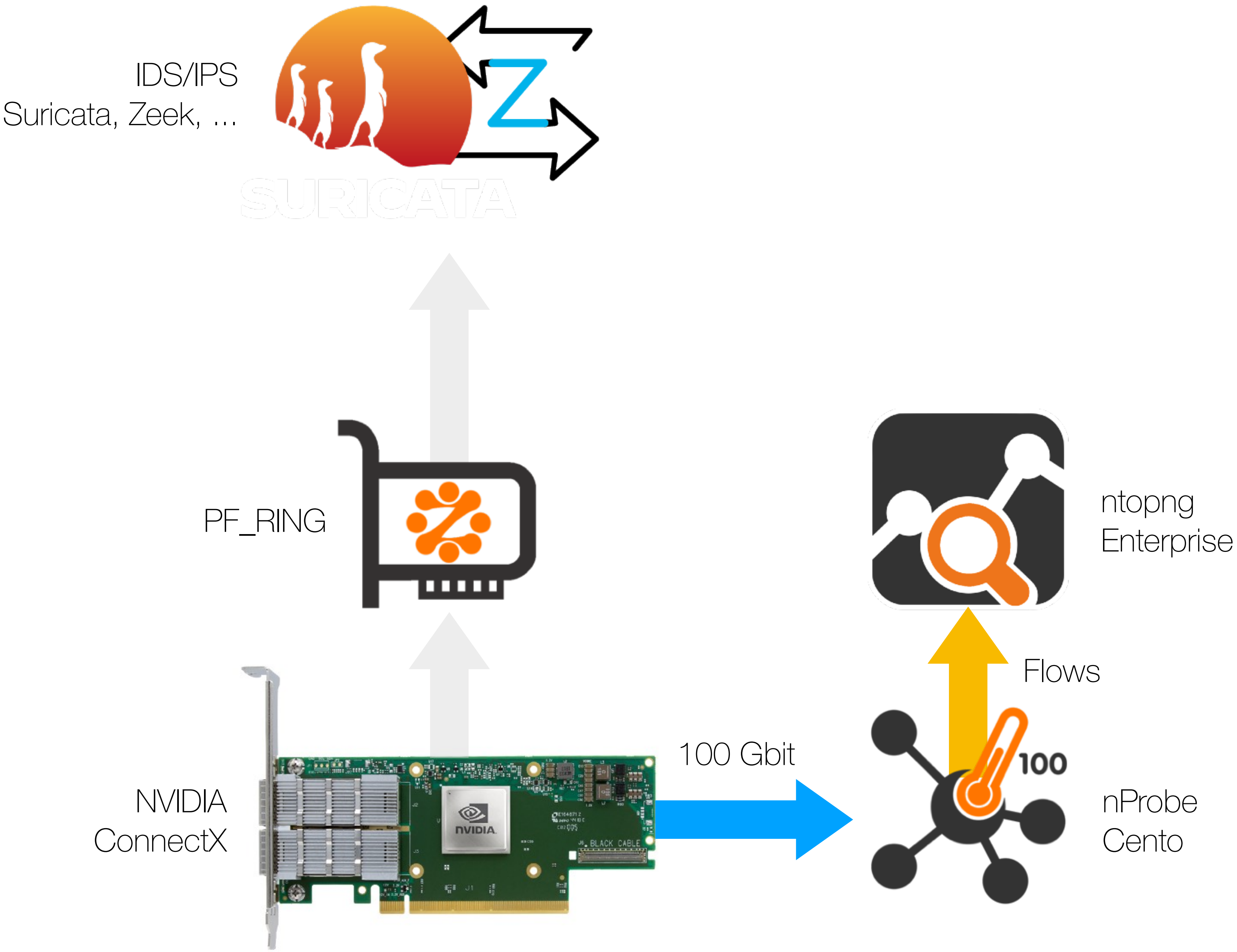
IDS/IPS
Suricata, Zeek, …

PF_RING

NVIDIA
ConnectX

ntopng
Enterprise

Suricata and Zeek On Demand



IDS/IPS
Suricata, Zeek, …

PF_RING

ntopng
Enterprise

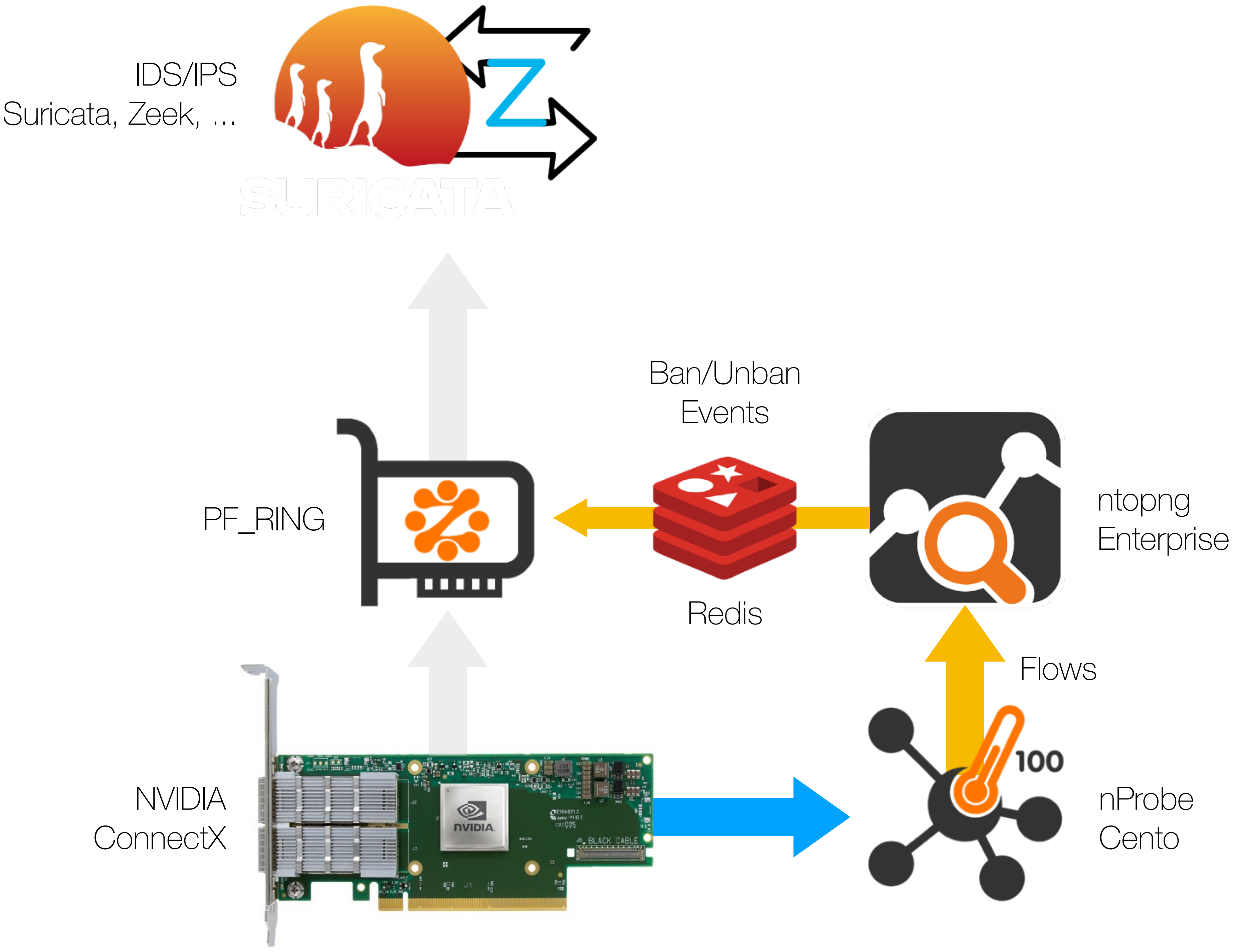
Flows

100 Gbit

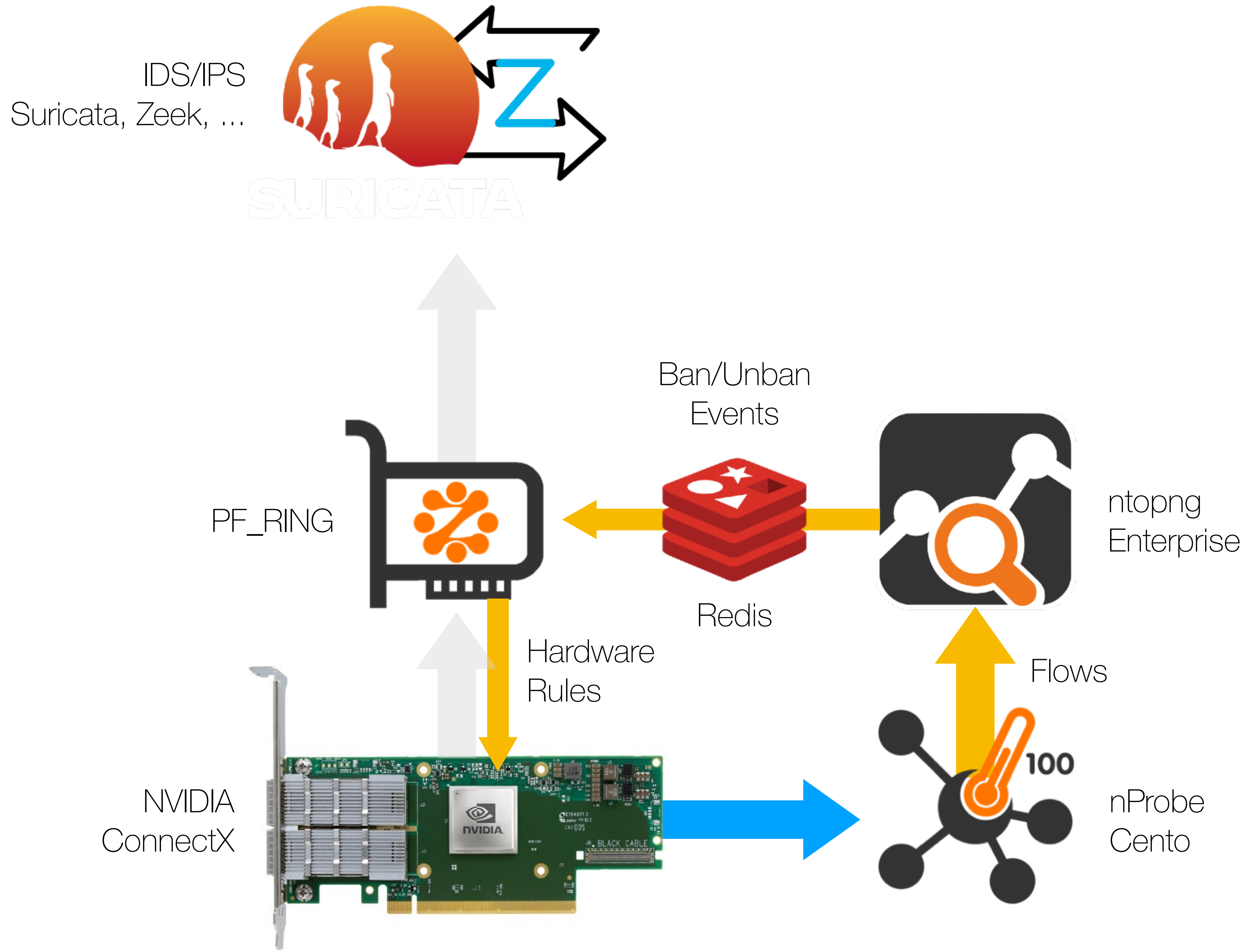
NVIDIA
ConnectX

nProbe
Cento

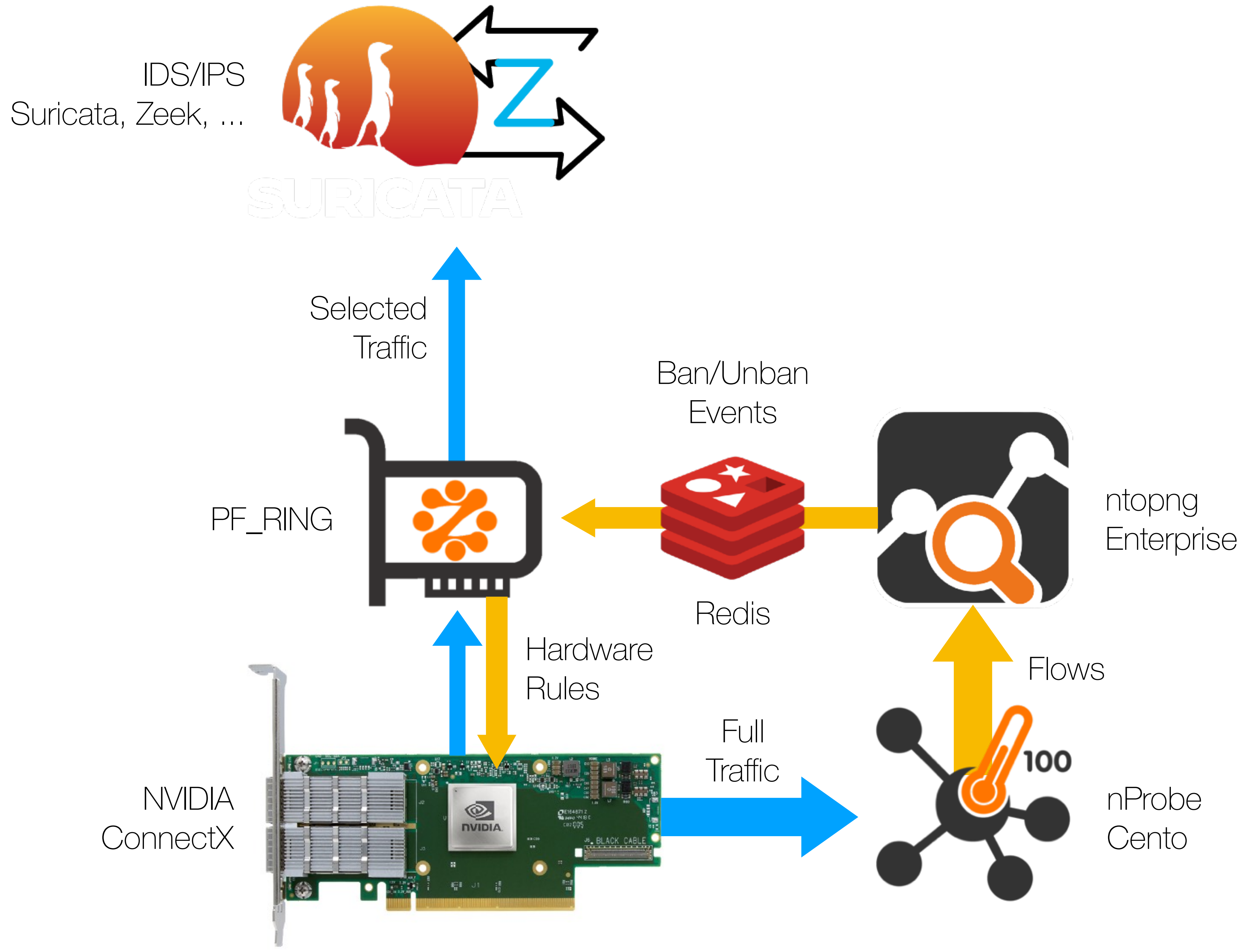
Suricata and Zeek On Demand



Suricata and Zeek On Demand



Suricata and Zeek On Demand



nBox UI

nBox Appliance

- A turnkey solution for those who don't want to bother with hardware selection, software installation and tuning

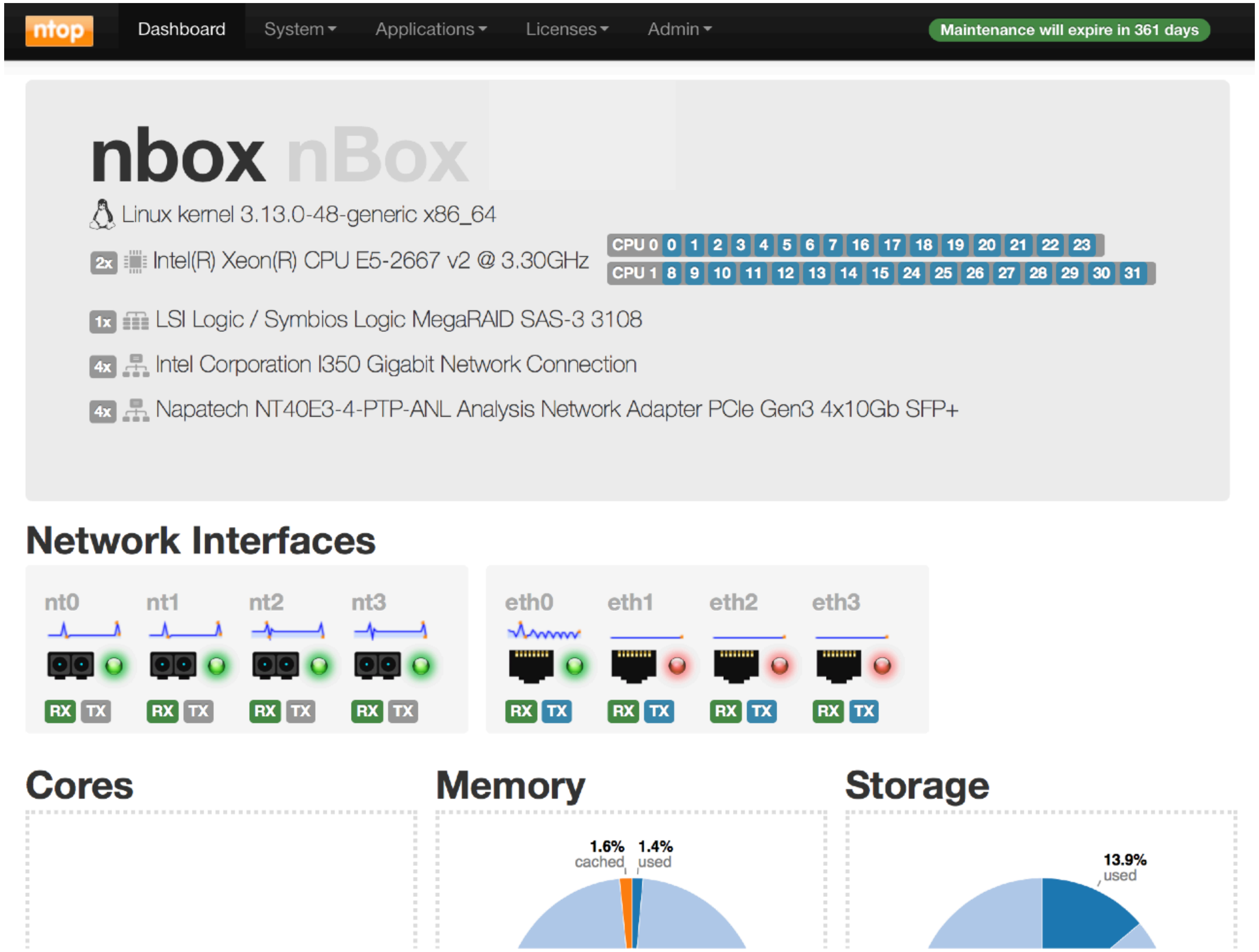
nBox NetFlow

with nProbe or nProbe Cento
and ntopng

nBox Recorder

with n2disk and disk2n

(Old) User Interface



nbox nBox

Linux kernel 3.13.0-48-generic x86_64

2x Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz

CPU 0 0 1 2 3 4 5 6 7 16 17 18 19 20 21 22 23

CPU 1 8 9 10 11 12 13 14 15 24 25 26 27 28 29 30 31

1x LSI Logic / Symbios Logic MegaRAID SAS-3 3108

4x Intel Corporation I350 Gigabit Network Connection

4x Napatech NT40E3-4-PTP-ANL Analysis Network Adapter PCIe Gen3 4x10Gb SFP+

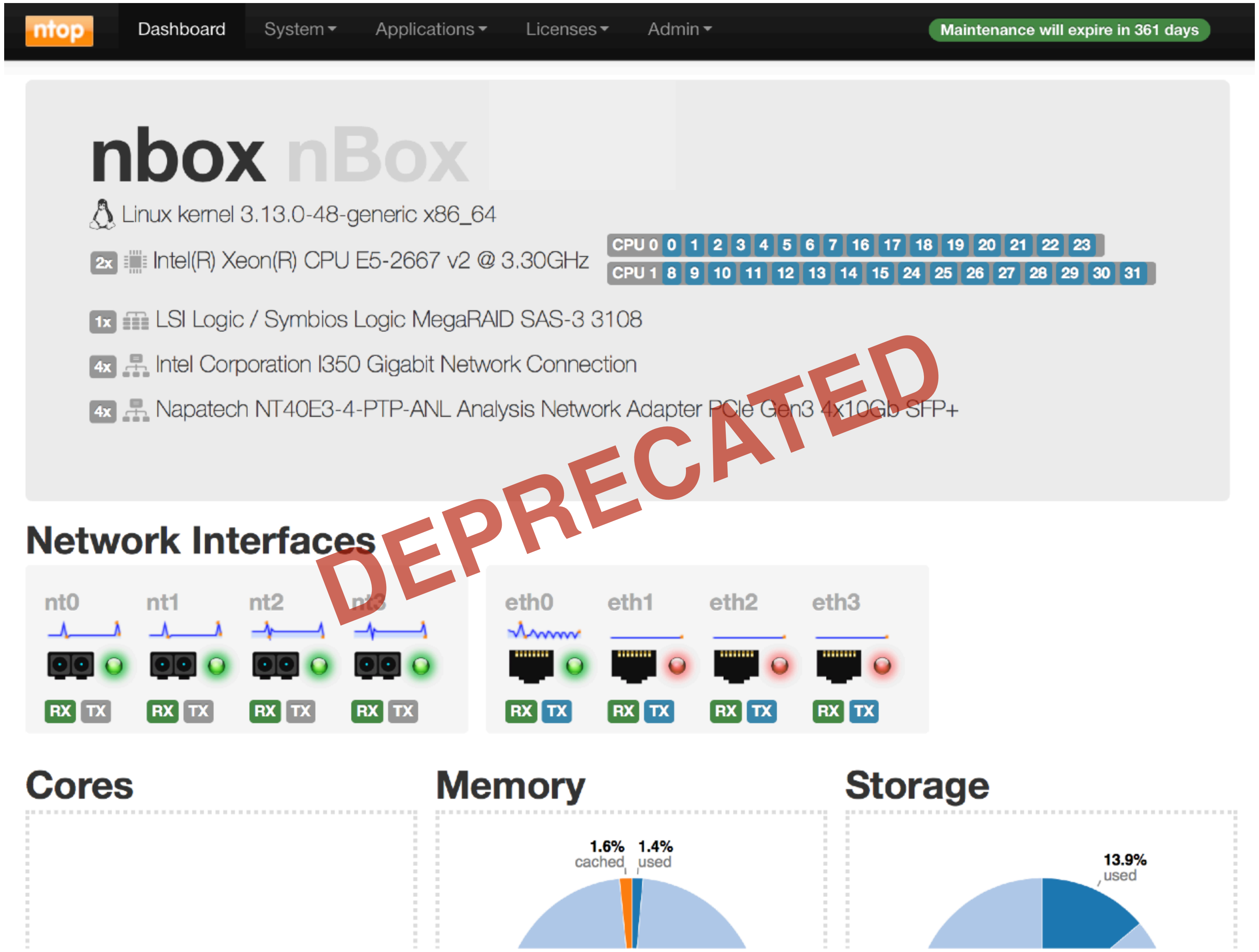
Network Interfaces

Cores

Memory

Storage

(Old) User Interface



nbox nBox

Linux kernel 3.13.0-48-generic x86_64

2x Intel(R) Xeon(R) CPU E5-2667 v2 @ 3.30GHz

CPU 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23

CPU 1 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31

1x LSI Logic / Symbios Logic MegaRAID SAS-3 3108

4x Intel Corporation I350 Gigabit Network Connection

4x Napatech NT40E3-4-PTP-ANL Analysis Network Adapter PCIe Gen3 4x10Gb SFP+

DEPRECATED

Network Interfaces

Cores

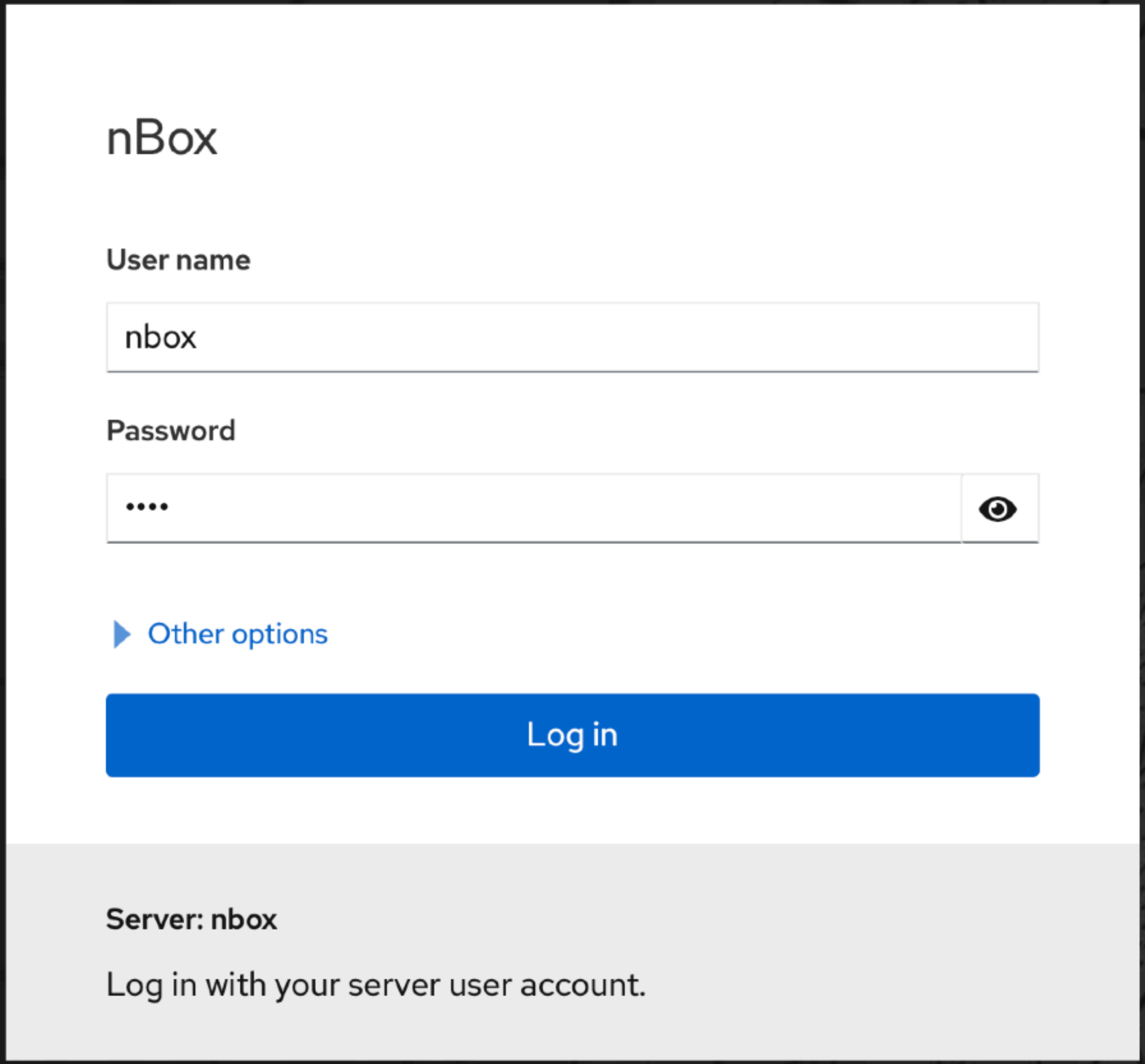
Memory

Storage

(Old) User Interface

- Supported on Ubuntu LTS only
  - Dependencies on the OS
- UI based on obsolete technologies
  - Perl-based CGI
  - HTML Templates
- Not easily extendable by the user
- It was time to rewrite it from scratch!

New nBox UI



nBox

User name

nbox

Password

••••

▶ Other options

Log in

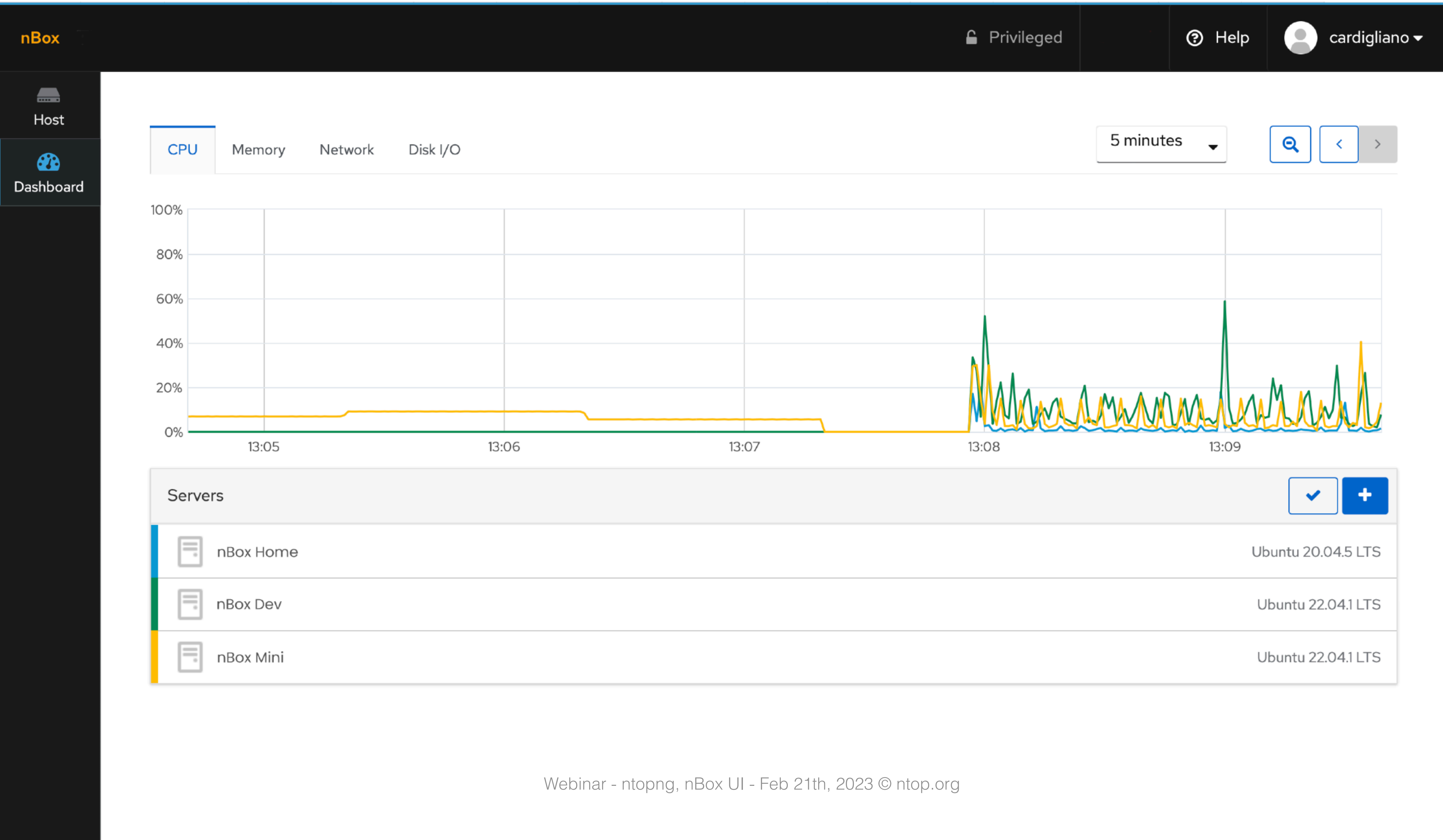
Server: nbox

Log in with your server user account.

New nBox UI

- Integrated in Cockpit, an Open Source web-based UI for servers sponsored by Red Hat
- Runs on most Linux distributions, including Ubuntu, Debian, RedHat
- Becoming a standard for managing Linux servers
- Extensible by means of plugins (Javascript API)
    - ntop plugins written in modern HTTP and Vue.js
    - Users can extend it

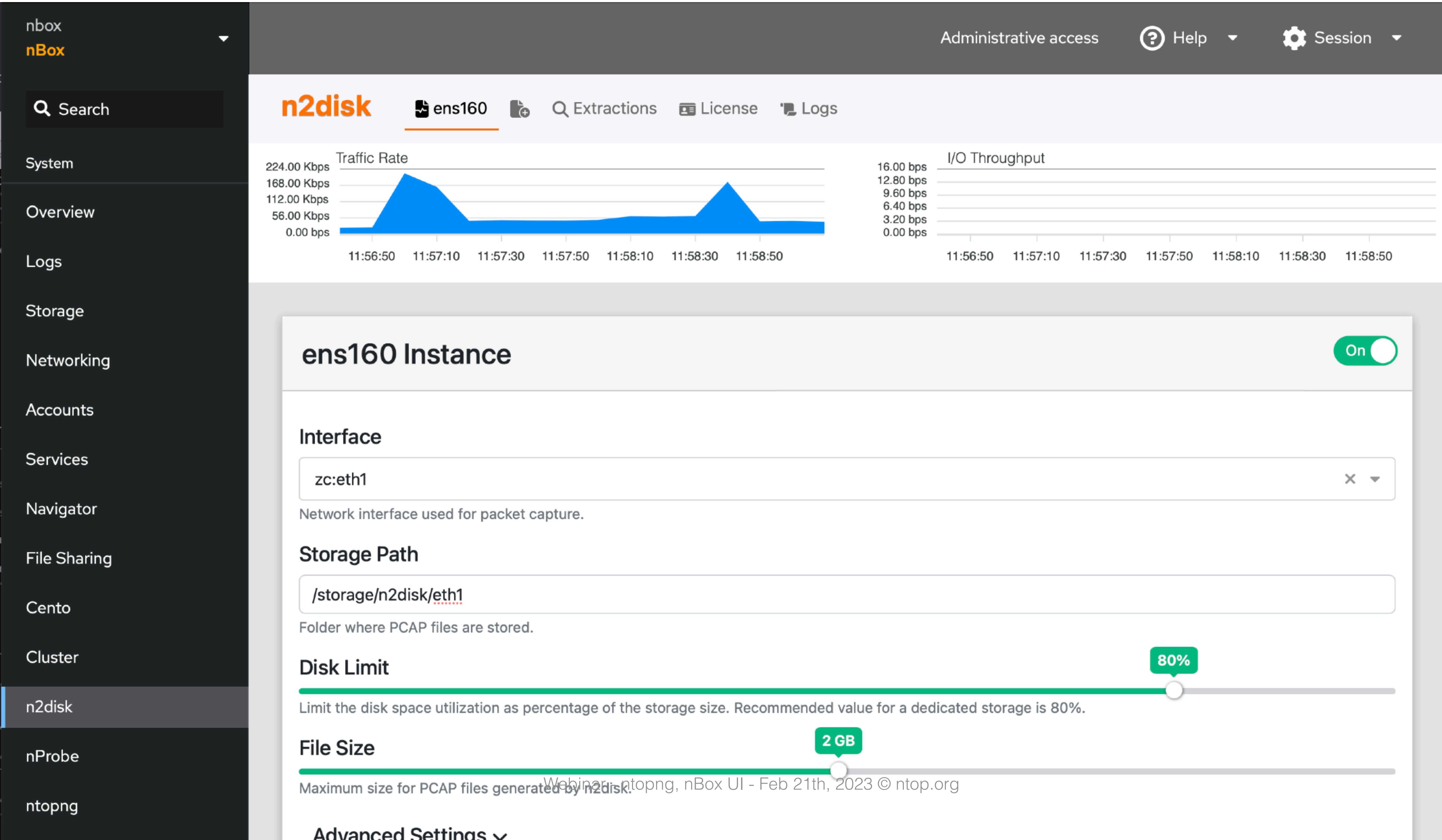
Monitor



Servers

nBox Home	Ubuntu 20.04.5 LTS
nBox Dev	Ubuntu 22.04.1 LTS
nBox Mini	Ubuntu 22.04.1 LTS

Control



ens160 Instance

Interface

zc:eth1

Network interface used for packet capture.

Storage Path

/storage/n2disk/eth1

Folder where PCAP files are stored.

Disk Limit

80%

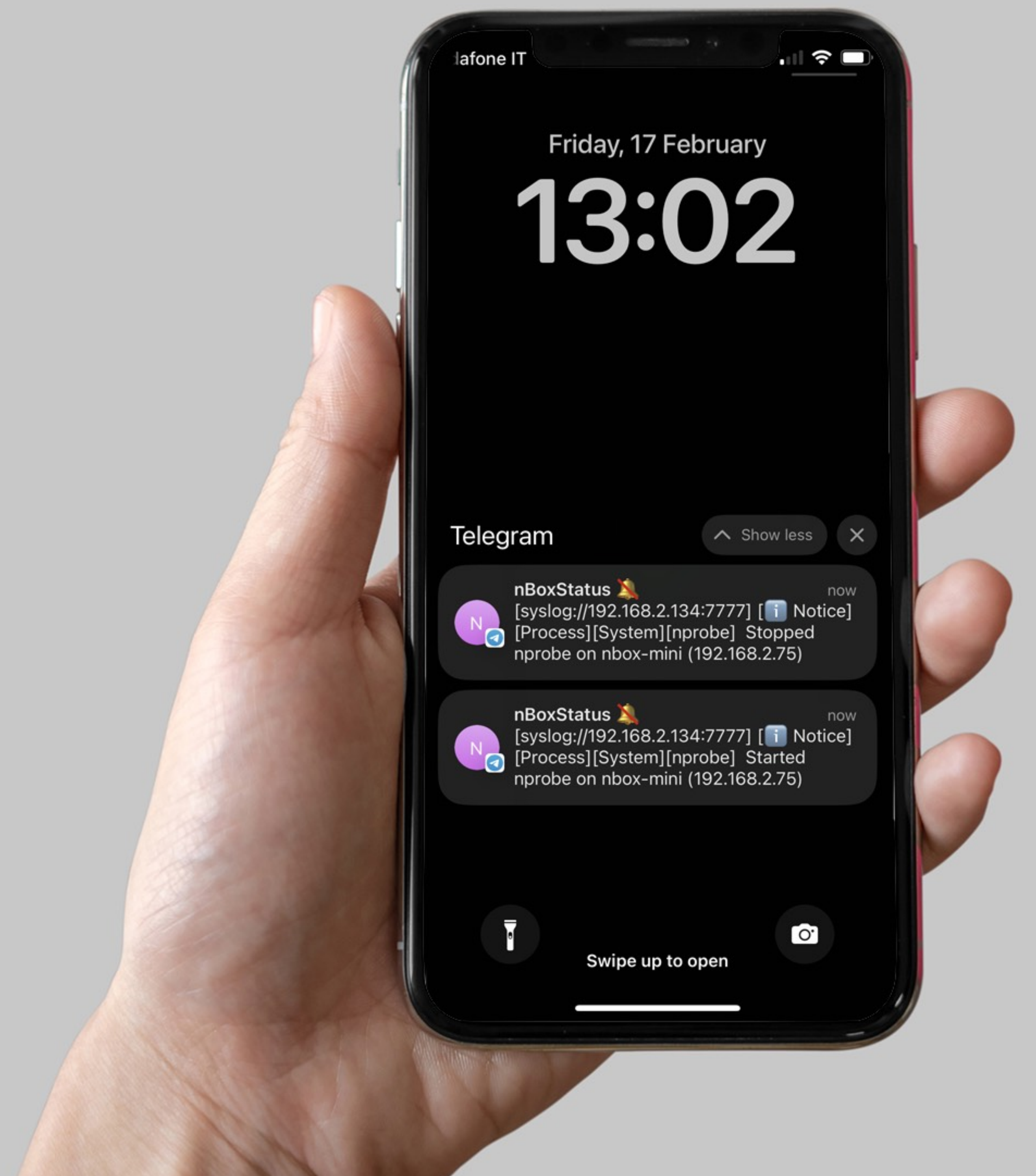
Limit the disk space utilization as percentage of the storage size. Recommended value for a dedicated storage is 80%.

File Size

2 GB

Maximum size for PCAP files generated by n2disk.

Notify



nBoxStatus 🔕 now
[syslog://192.168.2.134:7777] [ℹ️ Notice] [Process][System][nprobe] Stopped nprobe on nbox-mini (192.168.2.75)

nBoxStatus 🔕 now
[syslog://192.168.2.134:7777] [ℹ️ Notice] [Process][System][nprobe] Started nprobe on nbox-mini (192.168.2.75)

Thank you