

# NETWORK POLYGRAPH

## AN INNOVATIVE NETWORK VISIBILITY SERVICE (NOT ONLY) FOR NRENS

Pere Barlet-Ros<sup>1</sup>, Josep Sanjuas<sup>2</sup>, Josep Solé Pareta<sup>1</sup>, Maria Isabel Gandía<sup>3</sup>, Chelo Malagón<sup>4</sup>

<sup>1</sup> UPC-BarcelonaTech – {pbarlet, pareta}@ac.upc.edu <sup>2</sup> Talaia Networks – jsanjuas@talaiainetworks.com  
<sup>3</sup> CSUC – MariaIsabel.Gandia@csuc.cat <sup>4</sup> RedIRIS – chelo.malagon@rediris.es

### COMPANIES DEPEND ON NETWORKS

1. Productivity enhancement
2. Entire business models

### NETWORK MALFUNCTIONS ⇒ LARGE COSTS

42,000 \$/h to 5,600 \$/min (Gartner, Ponemon Institute)

### SOLUTION: NETWORK VISIBILITY

“When you can measure what you are speaking about, and express it in numbers, you know something about it.” – Lord Kelvin

- understand how the network is used
- identify bandwidth hogs
- detect unwanted applications
- detect anomalies & attacks
- investigate security incidents
- long-term network planning

### TRADITIONAL APPROACHES

#### Deep Packet Inspection (DPI): high visibility at high cost

- instrument network with hardware  $\times$
- capture & analyze every data packet  $\times$
- compute any metric of interest  $\checkmark$

#### NetFlow / IPFIX / sFlow: low visibility at low cost

- delegate capturing to routers/switches (standardized)  $\checkmark$
- no access to packet contents - only *traffic summaries*  $\times$
- aggregate results and present them to user  $\times$

### NETWORK POLYGRAPH

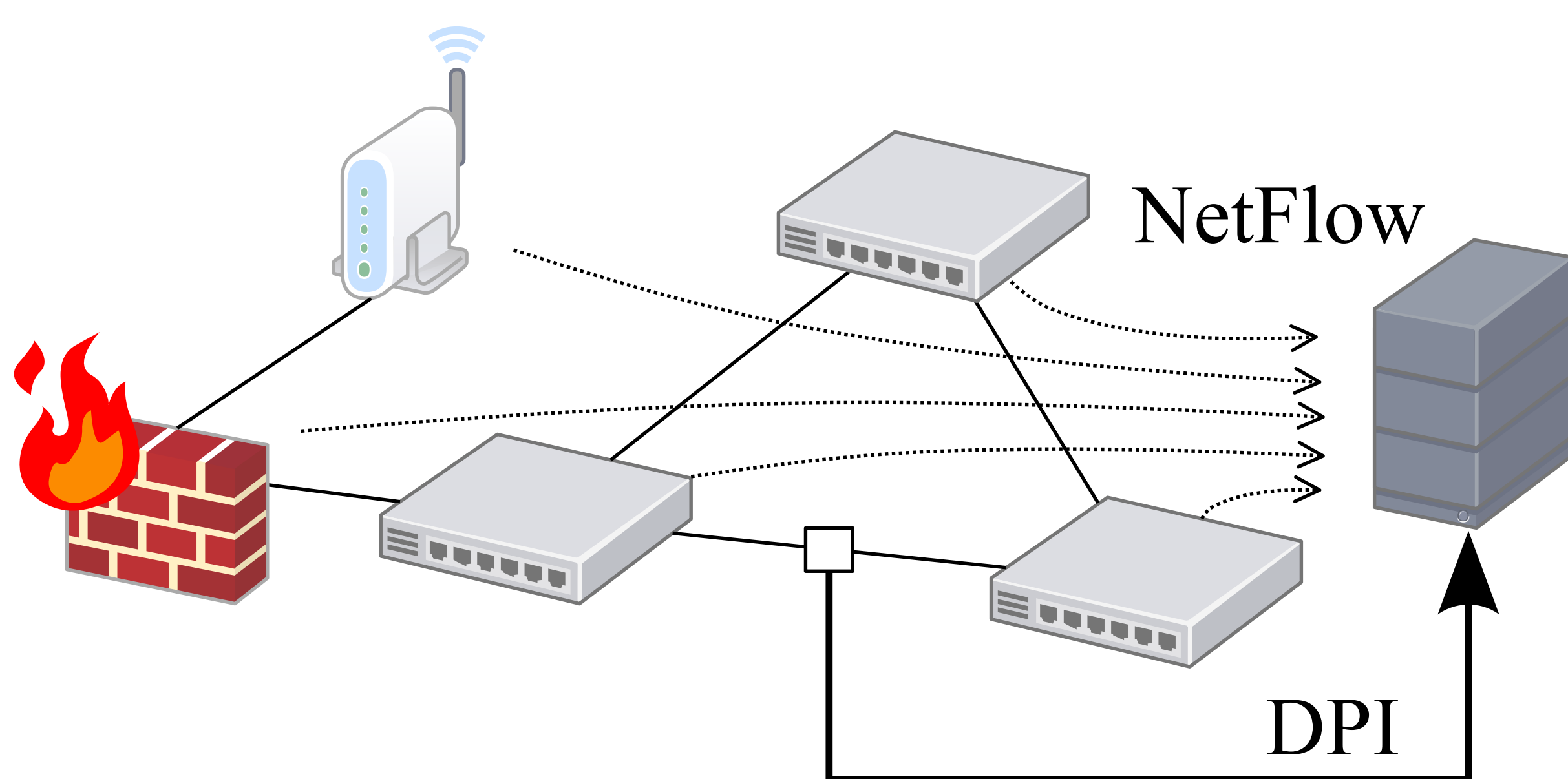
Leverages a huge body of research works in **traffic classification**, combines available techniques in a network visibility product

- **Capture** traffic at one link
- **Extract** NetFlow & perform DPI
- **Train** a classification engine
- **Extend** to *all* the network

Advantages:

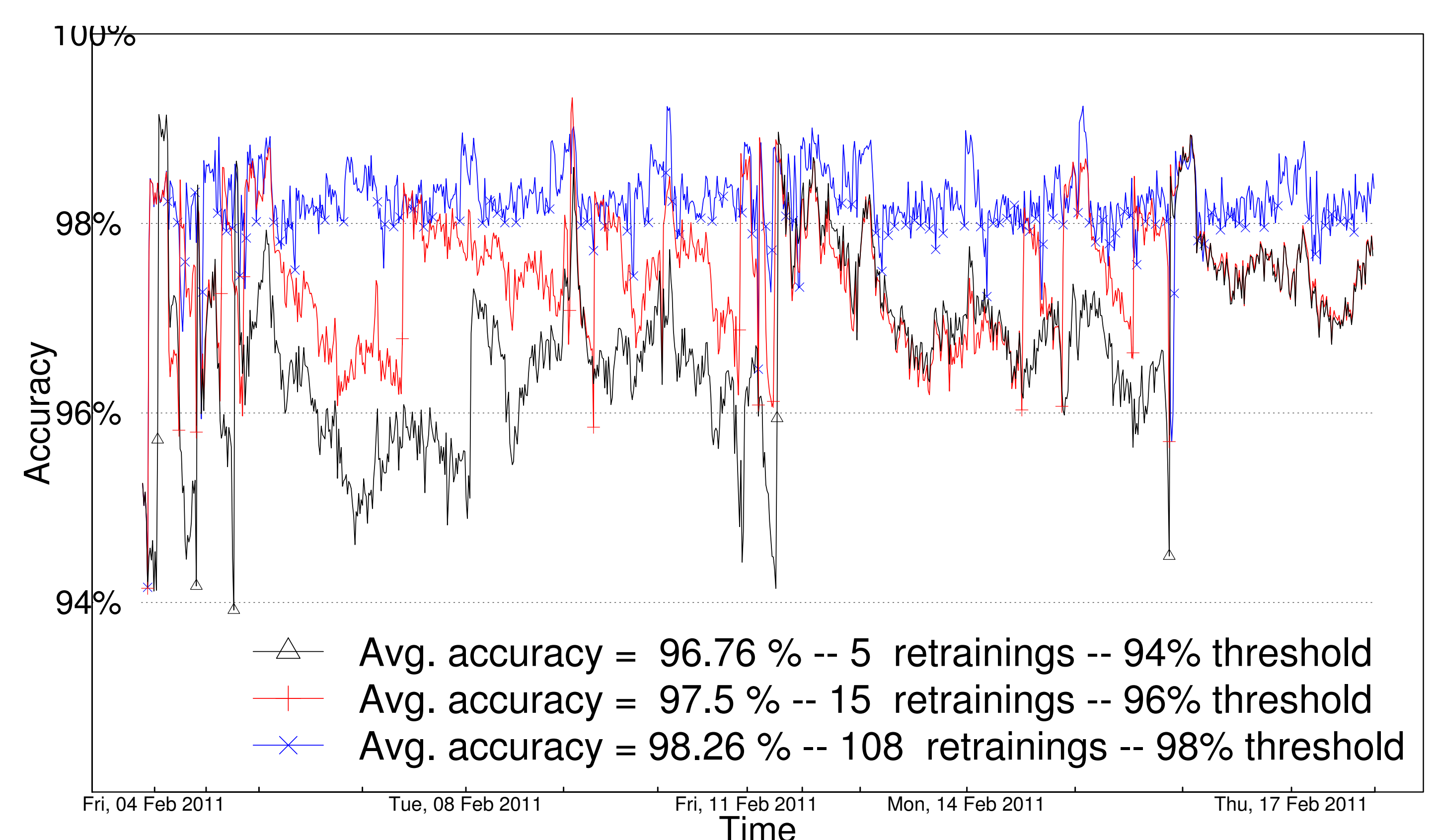
- $\checkmark$  Main data input: **NetFlow** – cost-effective, easy to deploy
- $\checkmark$  Accuracy comparable to DPI, ability to self-assess accuracy

### DEPLOYMENT AT CSUC AND REDIRIS

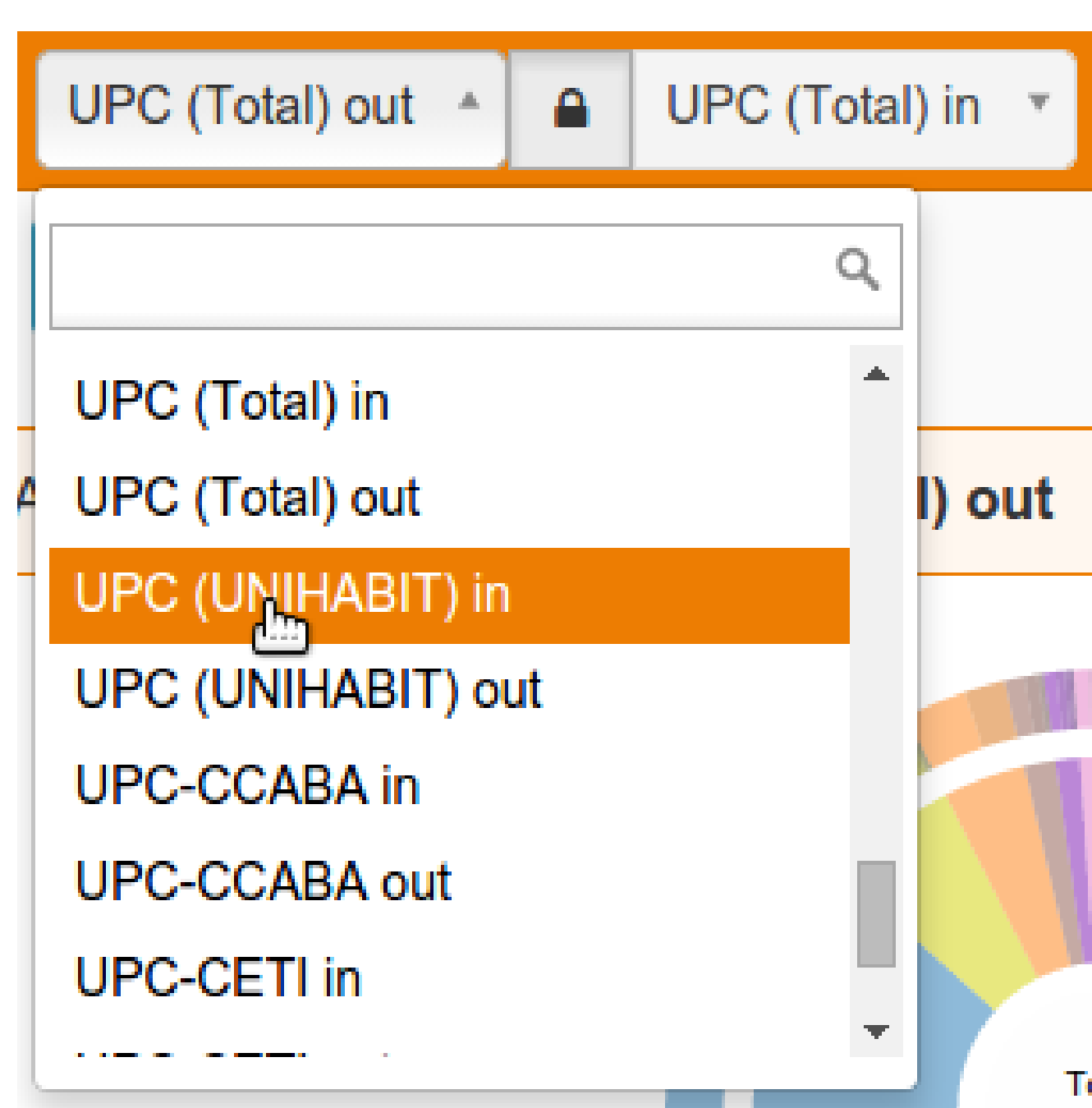


NetFlow as main data input. Auxiliary DPI input to train the application classification engine, which is applied to *all* the traffic.

### RESULTS



### MULTI-TENANT: SERVICES ALL INSTITUTIONS



Both an **internal tool** and a **value-added service** for institutions connected a NREN.

In production in Anella Científica (CSUC), and in deployment at RedIRIS (Red.es).

### CLOUD DEPLOYMENT

**Super fast deployment** (just a few minutes to configure routers).

Without DPI: runs on default lab-generated training model. Offered under a subscription model (SaaS) from the cloud. Currently in use by customers in 3 continents.

Offered by ourselves leveraging the multi-tenancy feature.

Alternatively, on-site deployment (possibly virtualized) is available.

On-line demo: <https://polygraph.io>