OCTOFLOW

NetFlows collector/filter/exporter/converter
using nprobe

Why

IFAD

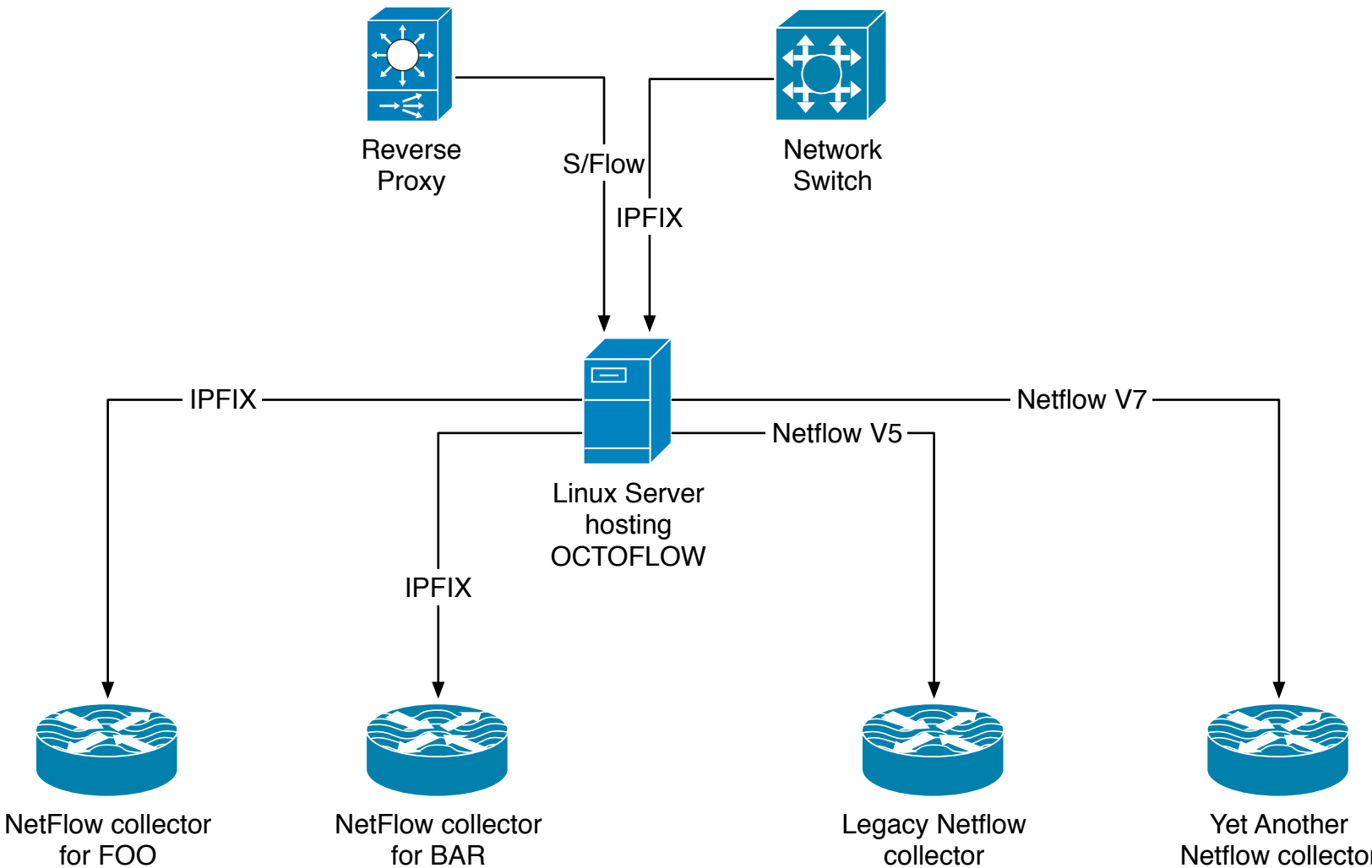
- NetFlows collection in shared infrastructure
- NetFlows are privacy-sensitive
- NetFlows need to be *filtered* and *replicated* to each customer collectors
- Shared infrastructure constraints make this not possible

How

IFAD

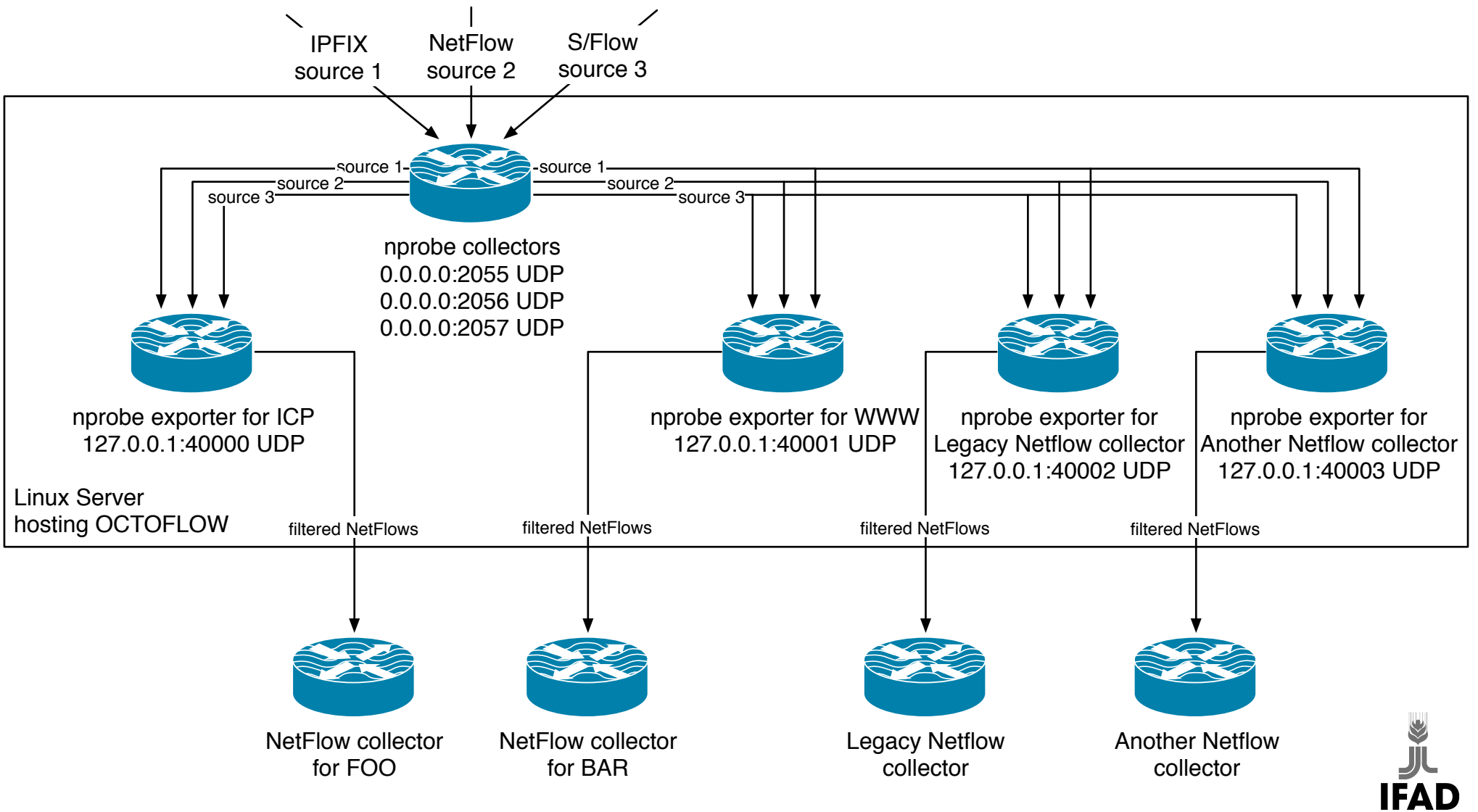
- Open Source to the rescue!
- **nprobe** is a Netflows collector, filterer, exporter and converter
- Multiple **nprobe** instances in a daisy chain, managed by a simple IFAD software
- Multiple customers can have their own NetFlows delivered to their own collectors

Infrastructure diagram



IFAD

Application diagram



IFAD

Architecture

IFAD

- Client/Server architecture
- Builds on python's *supervisord*
- Admin-friendly commands to start/status/stop
- Integrated with systemd
- Packaged as RPM
- HA-ready

Configuration

IFAD

General

```
general:
  conf_path: /etc/octoflow/confs          # Where config is stored
  systemd_path: /etc/systemd/system       # Where systemd units are

nprobe:
  bin_path: /usr/local/bin                # Full path to nprobe binary
  license_key: /path/to/license/key       # Full path to nprobe license

supervisor:
  supervisord_bin_path: /usr/bin          # Where supervisor is installed
  unix_socket: /tmp/octoflow.sock         # Full path to control socket
  logfile: /var/log/octoflow.log          # Full path to log file
  log_maxMB: 50                           # Max log file size before rotation
  log_max_backups: 10                     # Number of rotated logs to keep
  loglevel: debug                         # Log level
  autostart_instances: true               # Automatically start nprobes?
  autorestart_instances: true             # Restart nprobes if they crash?
  startretries_instances: 5               # How many times try to restart
```

Configuration

IFAD

Collectors

```
collectors:                     # NetFlow collectors list
  -
    id: 'cisco-switch'          # Collector identifier, used in command line
    listen_host: '0.0.0.0'      # Collector listen address
    listen_port: 2055           # Collector listen port
    nf_version: 10              # Collector NetFlow version accepted (IPFIX)
    mux_to:                     # Where to direct collected NetFlows
      - 'foo-cacti'             # Exporters list
      - 'bar-graylog'           #
      - 'nf-legacy'             #
      - 'nf-another'            #
  -
    id: 'reverse-proxy'         #
    listen_host: '0.0.0.0'      #
    listen_port: 2056           #
    nf_version: 'sflow'         #
    mux_to:                     #
      - 'foo-cacti'             #
      - 'bar-graylog'           #
```

Configuration

IFAD

Exporters

```
exporters:                                          # Exporters section list
  -
    id: 'foo-cacti'                                 # Exporter ID, used in command line
    listen_host: '127.0.0.1'                        # Exporter listen address
    listen_port: 40000                              # Exporter listen port
    collector_host: 192.168.0.101                   # Target collector address
    collector_port: 2055                            # Target collector port
    collector_proto: udp                            # Target collector protocol
    collector_version: 10                           # Target collector NetFlow version
    filters: ['10.0.1.0/24', '!10.0.1.254']         # Deliver NetFlows of 10.0.1.0/24 subnet but NOT
  -                                                 # ones for the 10.0.1.254 host
    id: 'bar-graylog'                               #
    listen_host: '127.0.0.1'                        #
    listen_port: 40001                              #
    collector_host: 10.3.37.11                      #
    collector_port: 2055                            #
    collector_proto: udp                            #
    collector_version: 10                           #
    filters: ['10.0.2.142', '10.0.2.139']           # Deliver Netflows of 10.0.2.142 & 10.0.2.139
  -
    id: 'nf-legacy'                                 #
    listen_host: '127.0.0.1'                        #
    listen_port: 40002                              #
    collector_host: 172.18.134.11                   #
    collector_port: 2055                            #
    collector_proto: udp                            #
    collector_version: 5                            #
    filters: ['172.16.0.0/12', '!172.17.1.0/24']    # Deliver Netflows of the 172.16.0.0/12 subnet with
                                                    # the exception of the 172.17.1.0/24 subnet
```

Usage

IFAD

Server

```
root@example.org:~/octoflow# python octoflow_server.py -h
usage: octoflow_server.py [-h] --config_file CONFIG_FILE

octoflow_server

optional arguments:
  -h, --help            show this help message and exit
  --config_file CONFIG_FILE
                        octoflow_server YAML configuration file.
```

Client

```
root@example.org:~/octoflow# python octoflow_client.py -h
usage: octoflow_client.py [-h] --config_file CONFIG_FILE
                          [--start START | --stop STOP | --status STATUS | --restart RESTART |
--reload | --reread | --shutdown]

octoflow_client

optional arguments:
  -h, --help            show this help message and exit
  --config_file CONFIG_FILE
                        octoflow_server YAML configuration file.
  --start START
  --stop STOP
  --status STATUS
  --restart RESTART
  --reload
  --reread
  --shutdown
```

Example

IFAD

- Start the daisy chain
- Get status
- Stop one instance
- Shutdown

```
root@example.org:~# python octoflow_server.py --config-file /etc/octoflow/octoflow.yaml
root@example.org:~# python octoflow_client.py --config-file /etc/octoflow/octoflow.yaml --status all
cisco-vswitch_collector    RUNNING pid 4173, uptime 0:00:07
reverse-proxy_collector    RUNNING pid 4175, uptime 0:00:07
foo-cacti_exporter         RUNNING pid 4172, uptime 0:00:07
bar-graylog_exporter       RUNNING pid 4174, uptime 0:00:07
nf-legacy_exporter         RUNNING pid 4176, uptime 0:00:07
nf-another_exporter        RUNNING pid 4178, uptime 0:00:07
root@example.org:~# python octoflow_client.py --config-file /etc/octoflow/octoflow.yaml --stop foo-
    cacti_exporter
foo-cacti_exporter: stopped
root@example.org:~# python octoflow_client.py --config-file /etc/octoflow/octoflow.yaml --status all
cisco-vswitch_collector    RUNNING pid 4173, uptime 0:00:12
reverse-proxy_collector    RUNNING pid 4175, uptime 0:00:12
foo-cacti_exporter         STOPPED Jun 12 11:42AM
bar-graylog_exporter       RUNNING pid 4174, uptime 0:00:12
nf-legacy_exporter         RUNNING pid 4176, uptime 0:00:12
nf-another_exporter        RUNNING pid 4178, uptime 0:00:12
root@example.org:~# python octoflow_client.py --config-file /etc/octoflow/octoflow.yaml --shutdown
Shut down
root@example.org:~# python octoflow_client.py --config-file /etc/octoflow/octoflow.yaml --status all
unix:///tmp/octoflow.sock no such file
```

Thank you!

IFAD | FIDA

Investing in rural people
Investir dans les populations rurales
Invertir en la población rural
الاستثمار في السكان الريفيين