Security .Days

<Prague.CZ>
<9-11 April 2024>

GÉANT

Modular transport layer solution for semi/automated protection of infrastructure, communities and users in CESNET3 network

Tom Kosnar

CESNET

kosnar@cesnet.cz

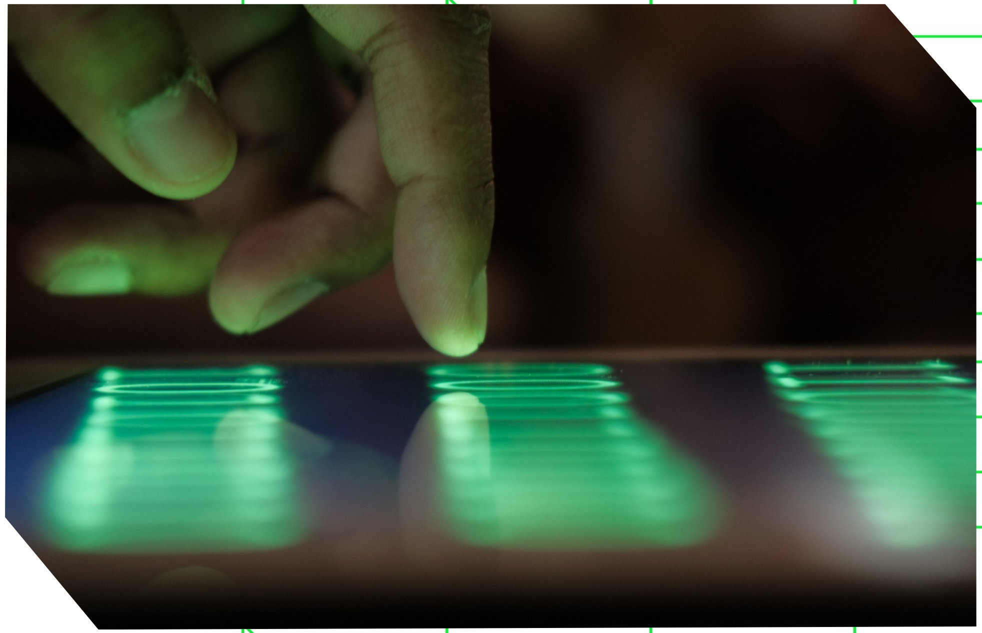
Co-funded by
the European Union

Motivation & Evolution

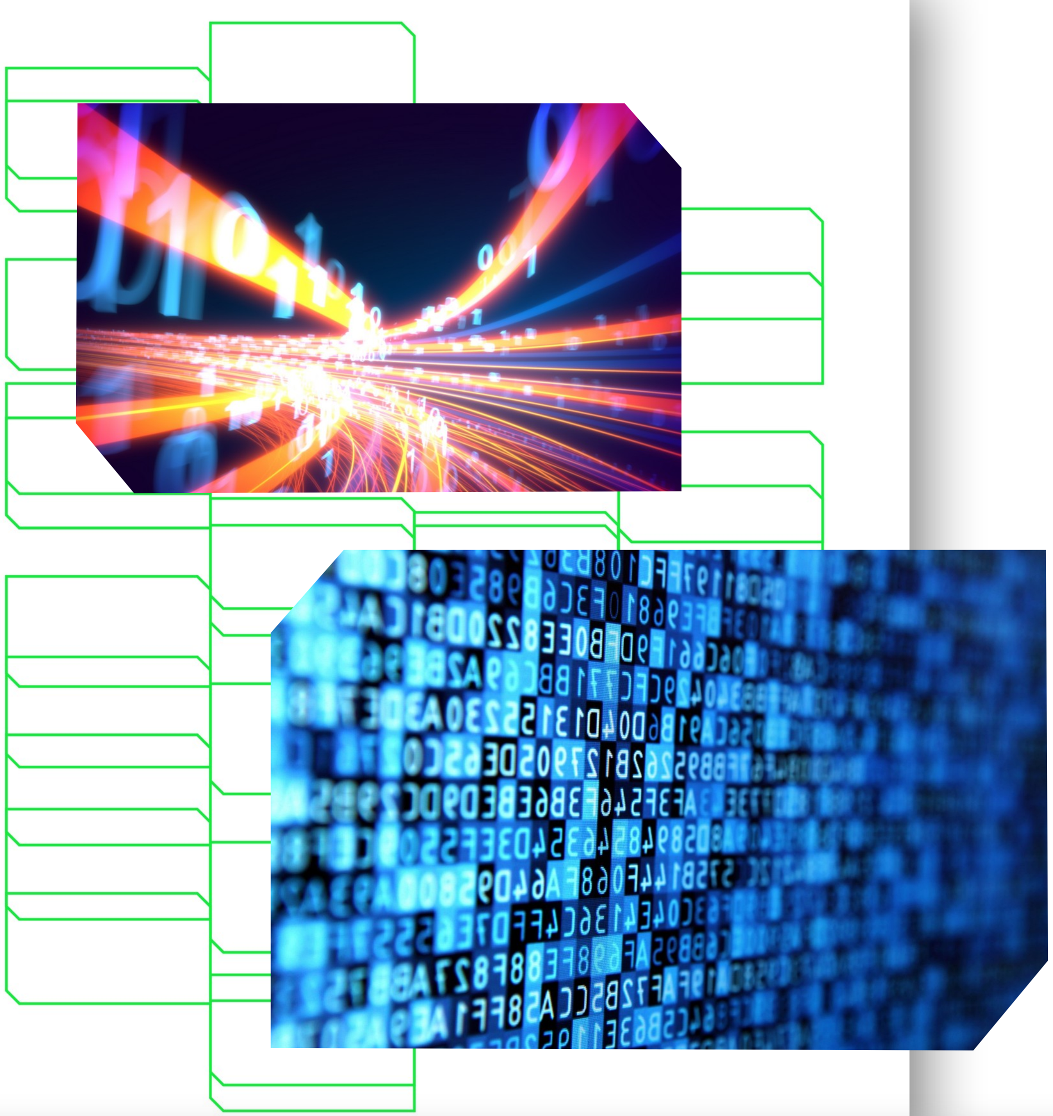
Automated transport layer protection

To keep infrastructure under control, protect users and save resources.. :-)

- wanted (years ago) to involve CSIRT more in network anomalies handling
- detection → notification → analysis → action
- ..amount of events NOT processable by humans & need to react faster
- automated system needed
- solution later extended to serve several use case types



Basic Building Blocks



Network (security) **setup**

- functions & services

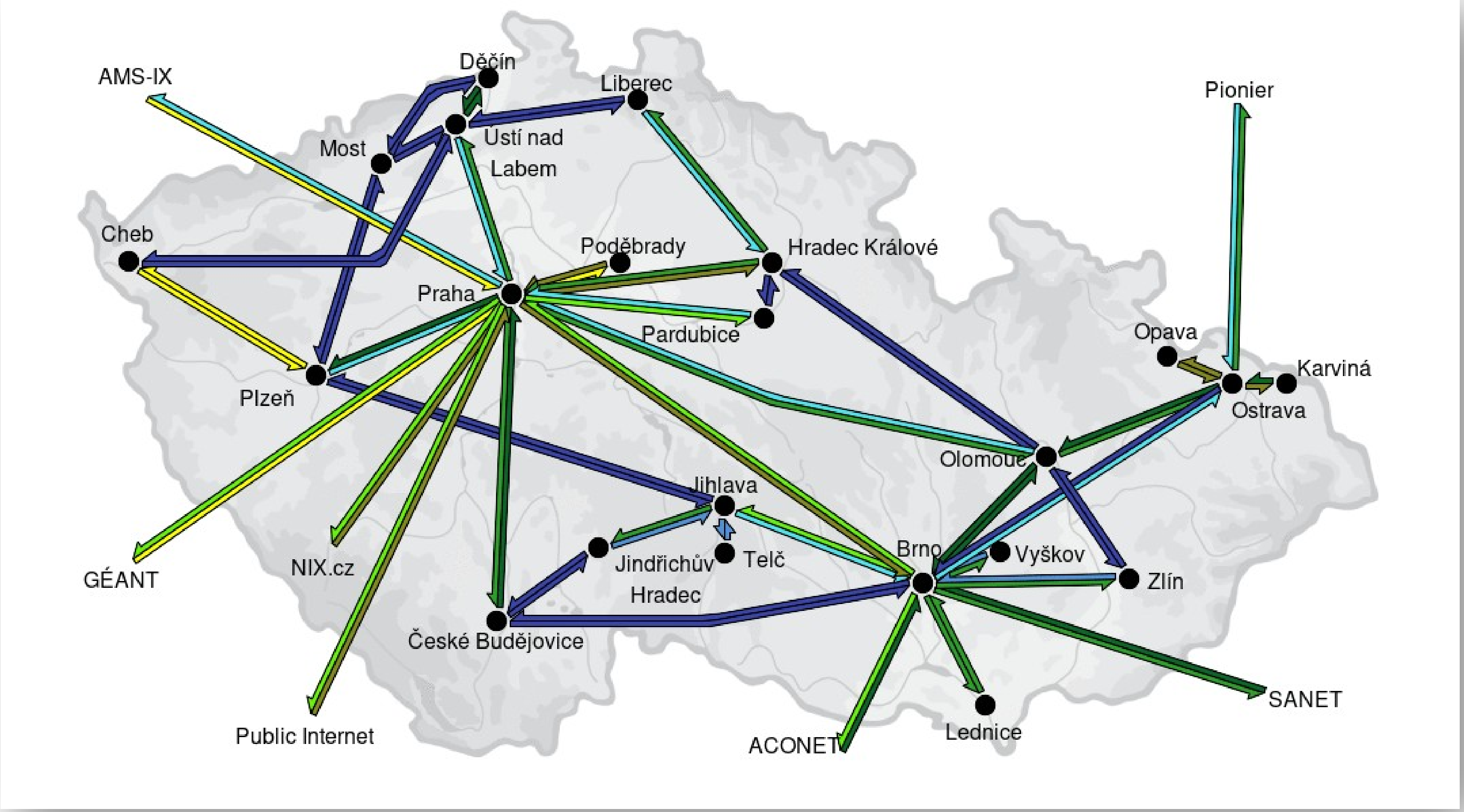
Tools

- traffic control
- monitoring & detections

Network Setup

CESNET3 network

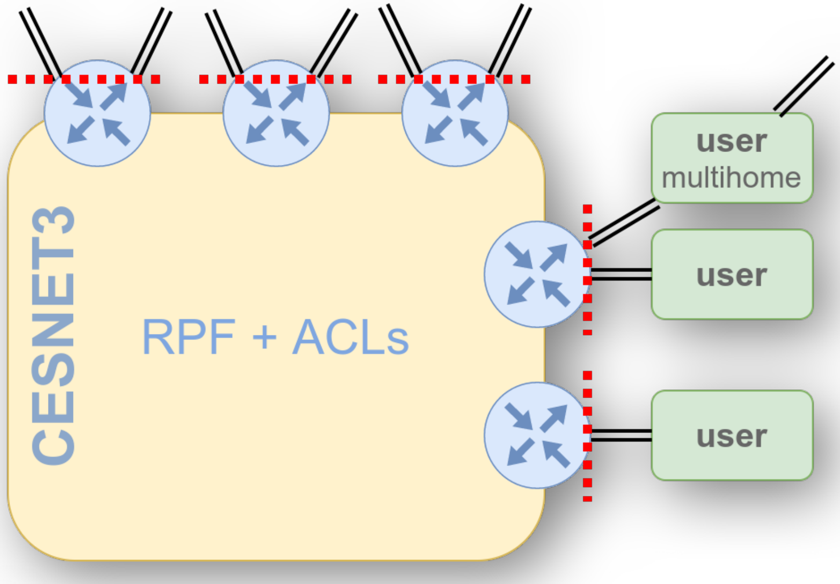
- multiple external paths
  - GÉANT
  - 3 cross-borders
  - 4 IXs
  - private peering
  - transit operator ~ 15% volume



Network Setup

1. ACL, Source IPs checks ~ *anti-spoofing*

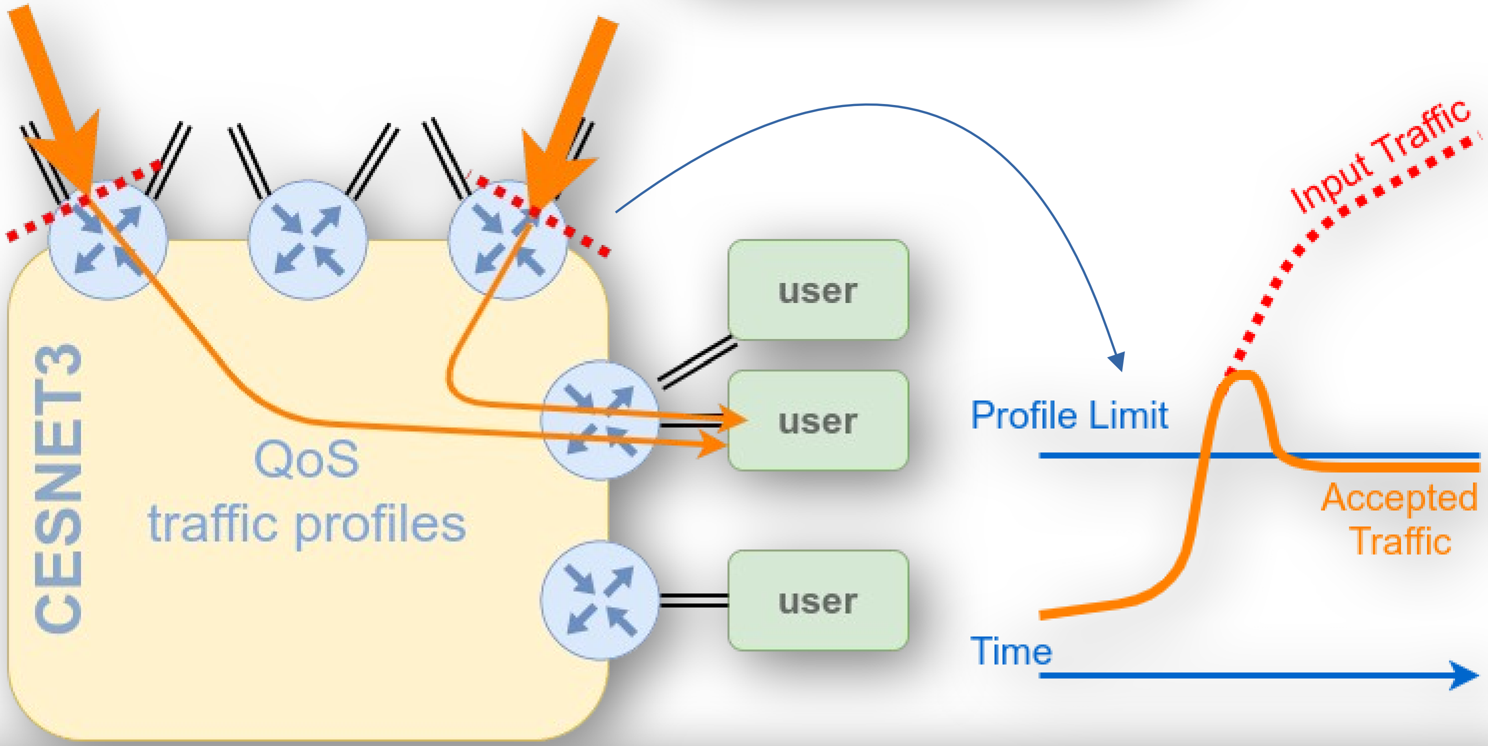
- BCP-38, RPF + ACLs



2. RPKI - Resource Public Key Infrastructure

3. QoS - traffic profiles

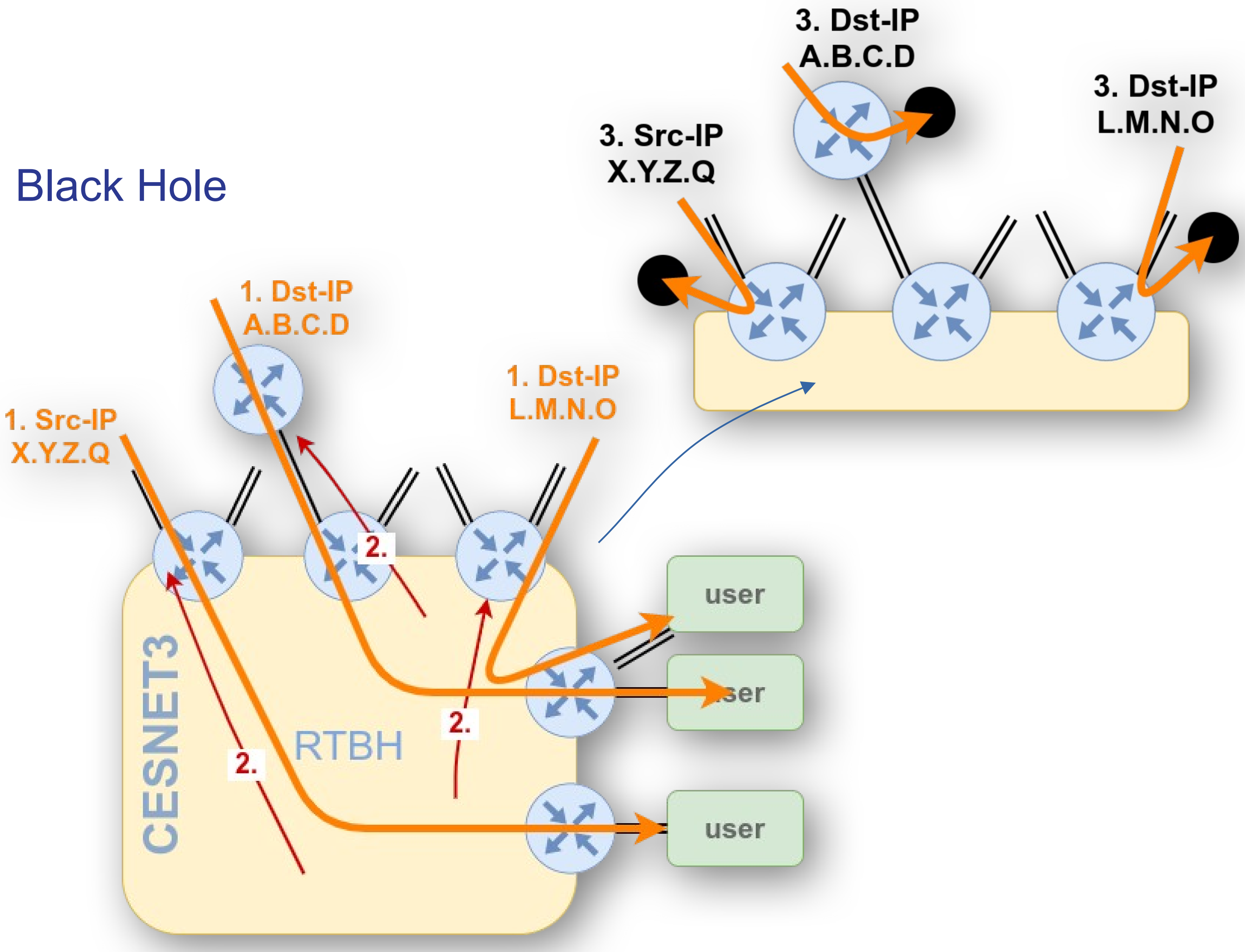
- catches 1st amplification waves
- key services – prefix based profiles
- ordinary services - AS wide profiles



Network Setup

4. RTBH - Remotely Triggered Black Hole

- external
  - external line protection
  - cooperation with external partners
- internal
  - whole backbone
  - destination + source



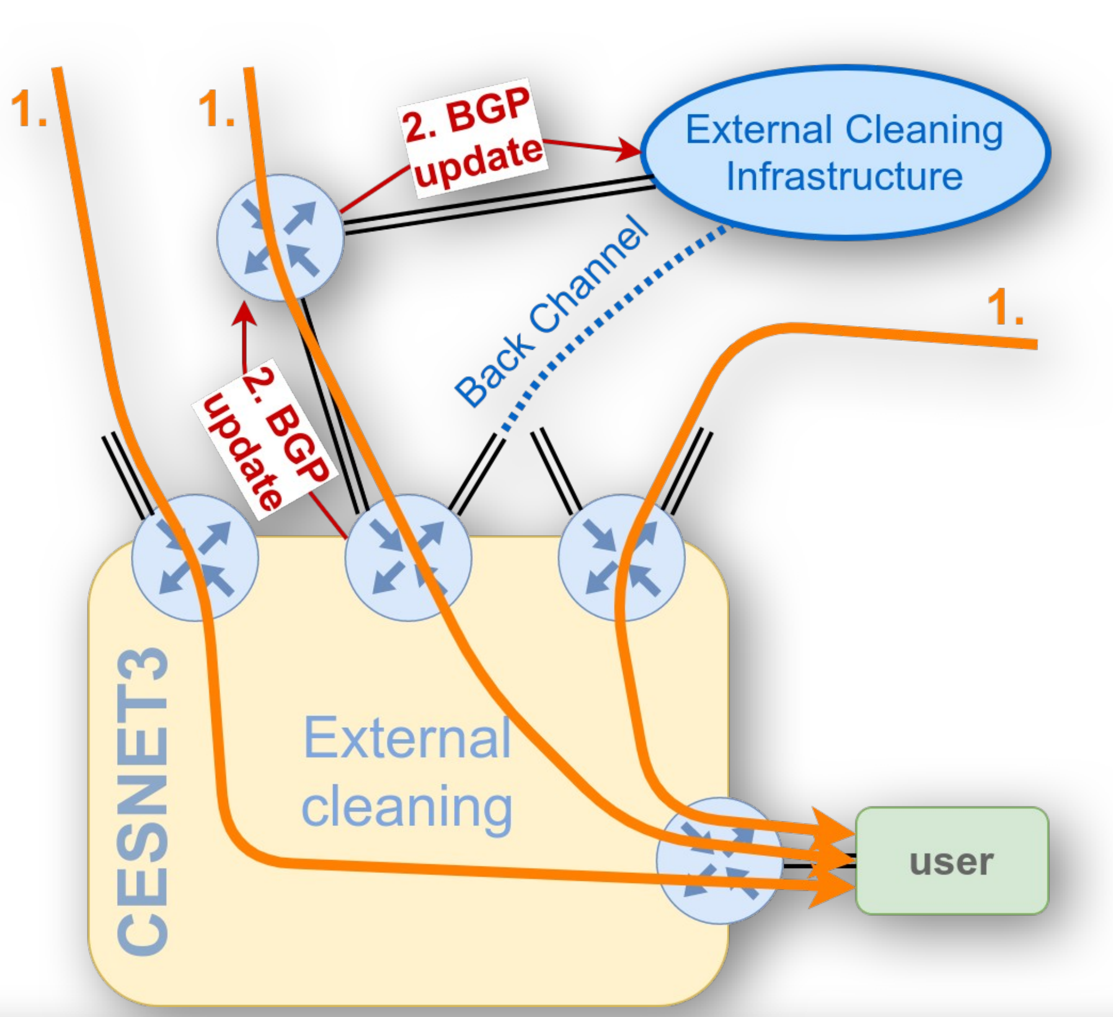
Network Setup

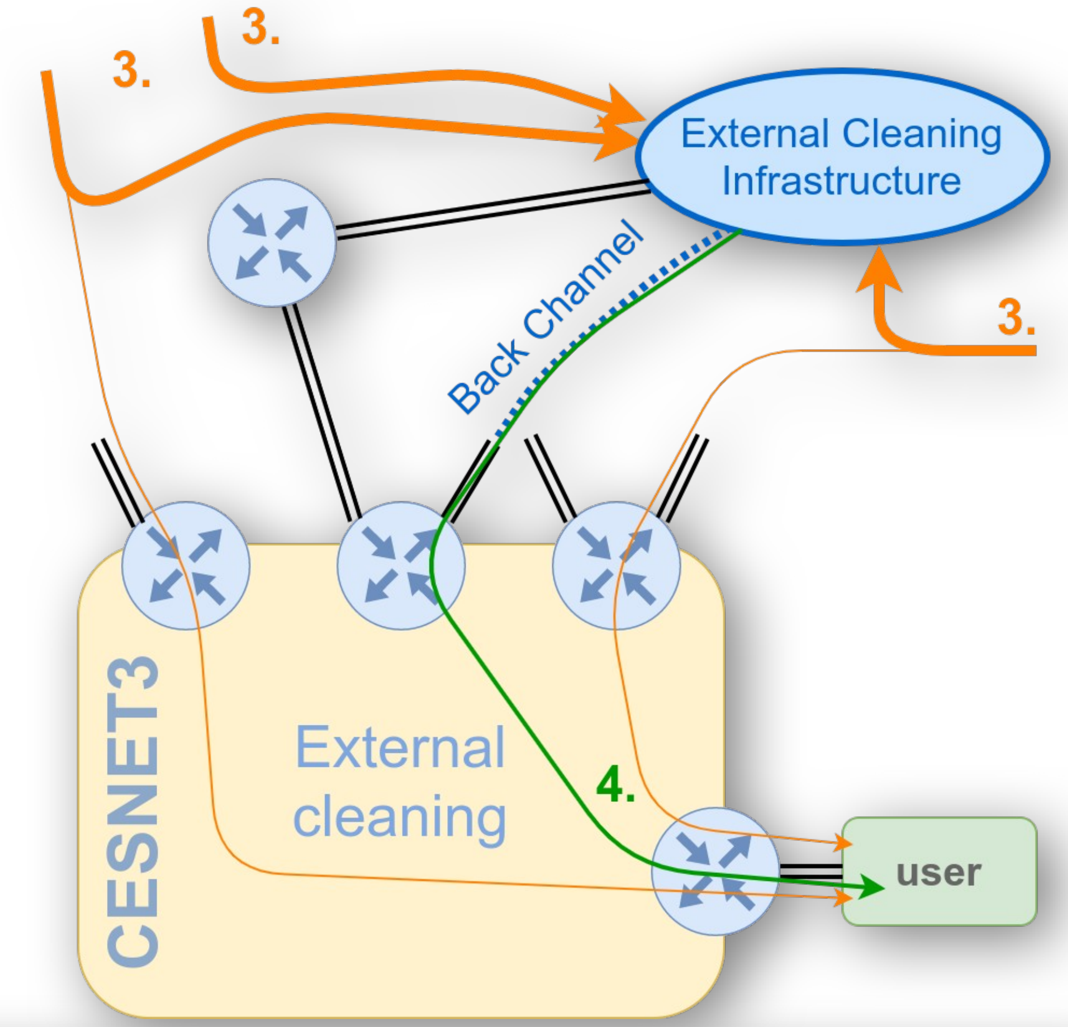
5. BGP FlowSpec

- more specific (flow-based) traffic selection (unlike RTBH ~ prefixes only)
- set of flow descriptive parameters → defined order
  - `Dst-Prefix, Src-Prefix, Protocol, Dst-Port, Src-Port, ICMP Type, ICMP Code, TCP Flags, Pkt-Length, DSCP, Fragment Encoding`
- action applied on matching traffic
  - `rate (incl. 0), traffic-action (sampling), redirect, marking`
- processing order given by ”**more specific**” **flow specification**

Network Setup

6. External traffic cleaning service - routing based control (multiple external paths)



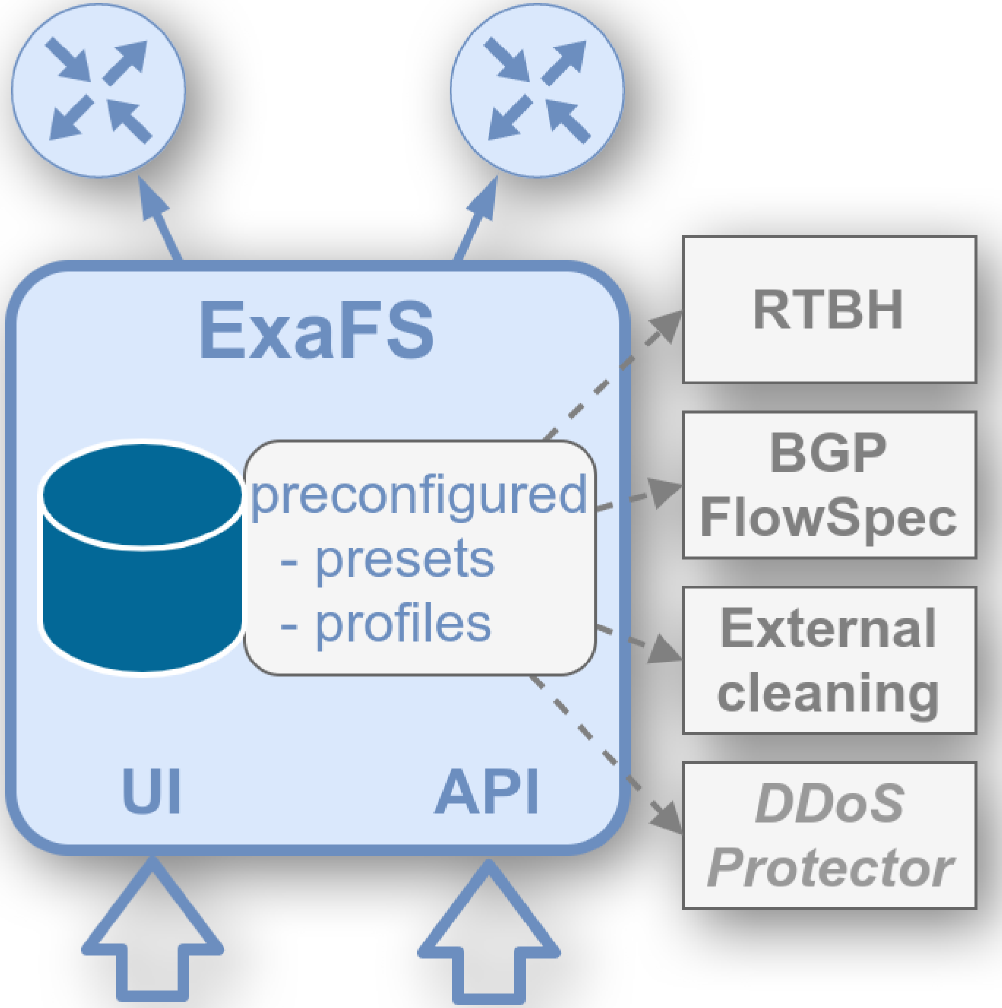


Tools

https://github.com/CESNET/exafs

ExaFS – essential tool

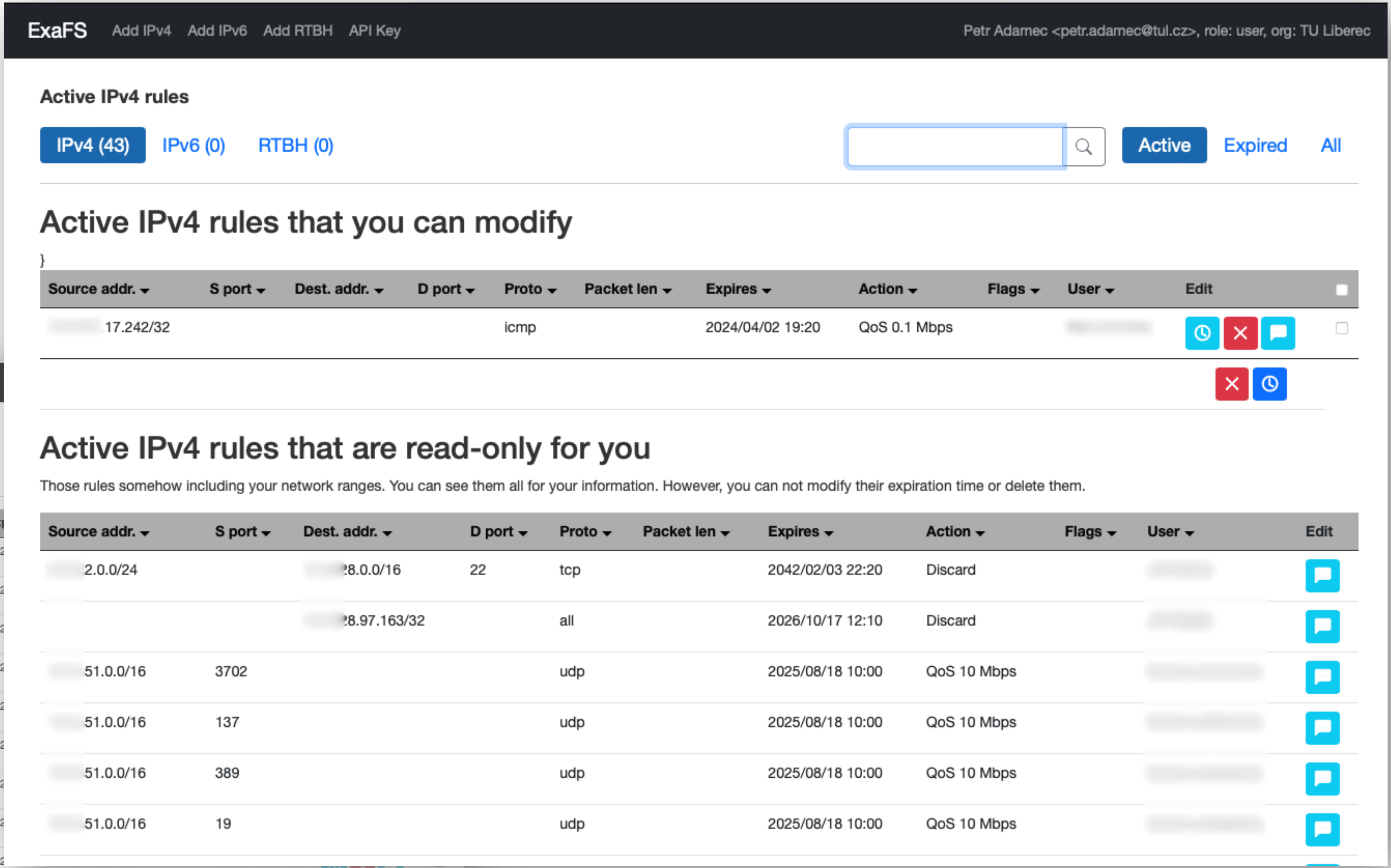
- **network traffic control tool** (routing information based)
- **single point of knowledge** → everything what is currently set up
- UI + API
- originally FlowSpec + RTBH (incl. traffic redirections and limitations)
- preconfigured set of rules (RTBH) and traffic profiles (FlowSpec)
- + new *DDoS protector*
- “prefix based” user authorization → as a service for connected networks



Tools

ExaFS UI example

- IPv4 FS dashboard



Petr Adamec <petr.adamec@tul.cz>, role: user, org: TU Liberec

Active IPv4 rules

IPv4 (43) IPv6 (0) RTBH (0)

Active Expired All

Active IPv4 rules that you can modify

}

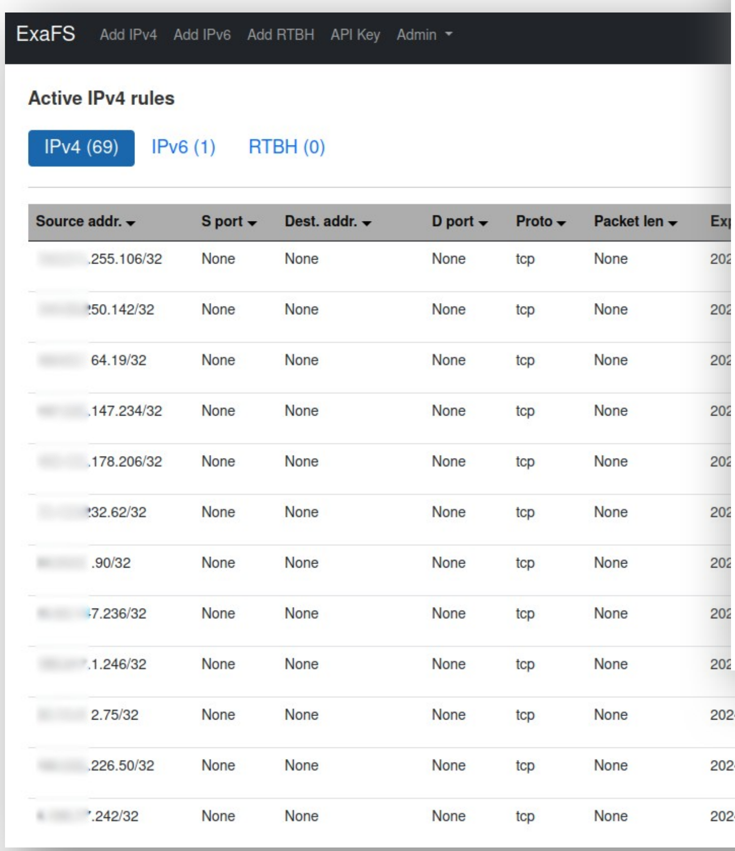
Source addr.	S port	Dest. addr.	D port	Proto	Packet len	Expires	Action	Flags	User	Edit	☐
[redacted]17.242/32				icmp		2024/04/02 19:20	QoS 0.1 Mbps		[redacted]	⏲ ✕ 💬	☐

✕ ⏲

Active IPv4 rules that are read-only for you

Those rules somehow including your network ranges. You can see them all for your information. However, you can not modify their expiration time or delete them.

Source addr.	S port	Dest. addr.	D port	Proto	Packet len	Expires	Action	Flags	User	Edit
[redacted]2.0.0/24		[redacted]8.0.0/16	22	tcp		2042/02/03 22:20	Discard		[redacted]	💬
		[redacted]8.97.163/32		all		2026/10/17 12:10	Discard		[redacted]	💬
[redacted]51.0.0/16	3702			udp		2025/08/18 10:00	QoS 10 Mbps		[redacted]	💬
[redacted]51.0.0/16	137			udp		2025/08/18 10:00	QoS 10 Mbps		[redacted]	💬
[redacted]51.0.0/16	389			udp		2025/08/18 10:00	QoS 10 Mbps		[redacted]	💬
[redacted]51.0.0/16	19			udp		2025/08/18 10:00	QoS 10 Mbps		[redacted]	💬



Active IPv4 rules

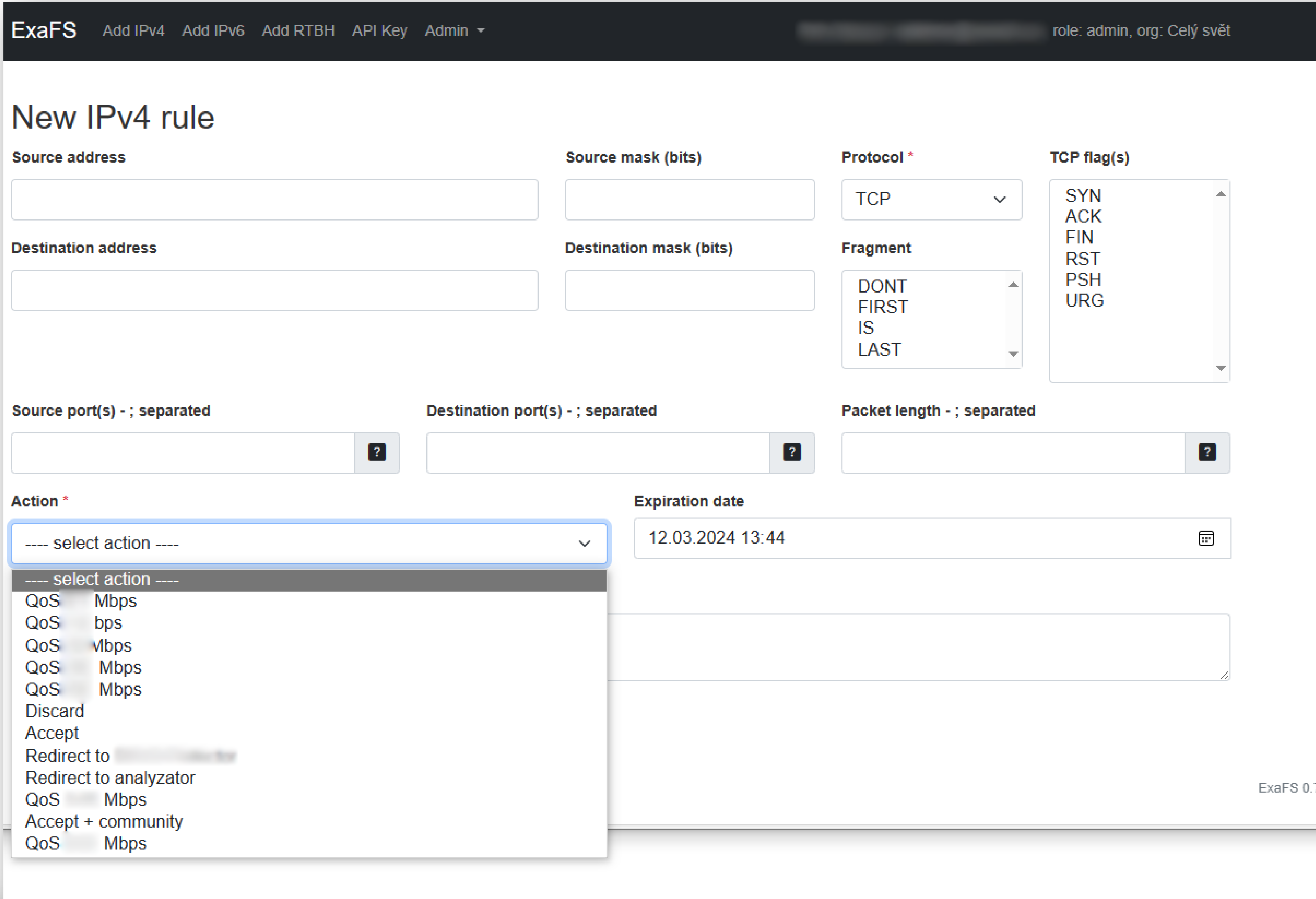
IPv4 (69) IPv6 (1) RTBH (0)

Source addr.	S port	Dest. addr.	D port	Proto	Packet len	Exp					
[redacted].255.106/32	None	None	None	tcp	None	202					
[redacted]250.142/32	None	None	None	tcp	None	202					
[redacted]64.19/32	None	None	None	tcp	None	202					
[redacted].147.234/32	None	None	None	tcp	None	202					
[redacted].178.206/32	None	None	None	tcp	None	202					
[redacted]32.62/32	None	None	None	tcp	None	202					
[redacted].90/32	None	None	None	tcp	None	202					
[redacted]7.236/32	None	None	None	tcp	None	202					
[redacted].1.246/32	None	None	None	tcp	None	202					
[redacted]2.75/32	None	None	None	tcp	None	2024/03/20 16:30	Discard		Tomáš Košňar	⏲ ✕ 💬	☐
[redacted].226.50/32	None	None	None	tcp	None	2024/03/20 16:30	Discard		Tomáš Košňar	⏲ ✕ 💬	☐
[redacted].242/32	None	None	None	tcp	None	2024/03/20 16:20	Discard		Tomáš Košňar	⏲ ✕ 💬	☐

Tools

ExaFS UI example

- IPv4 FlowSpec rule form



ExaFS Add IPv4 Add IPv6 Add RTBH API Key Admin [redacted] role: admin, org: Celý svět

New IPv4 rule

Source address

Source mask (bits)

Protocol *

TCP

TCP flag(s)

SYN
ACK
FIN
RST
PSH
URG

Destination address

Destination mask (bits)

Fragment

DONT
FIRST
IS
LAST

Source port(s) - ; separated ?

Destination port(s) - ; separated ?

Packet length - ; separated ?

Action *

---- select action ----

---- select action ----
QoS [redacted] Mbps
QoS [redacted] bps
QoS [redacted] Mbps
QoS [redacted] Mbps
QoS [redacted] Mbps
Discard
Accept
Redirect to [redacted]
Redirect to analyzator
QoS [redacted] Mbps
Accept + community
QoS [redacted] Mbps

Expiration date

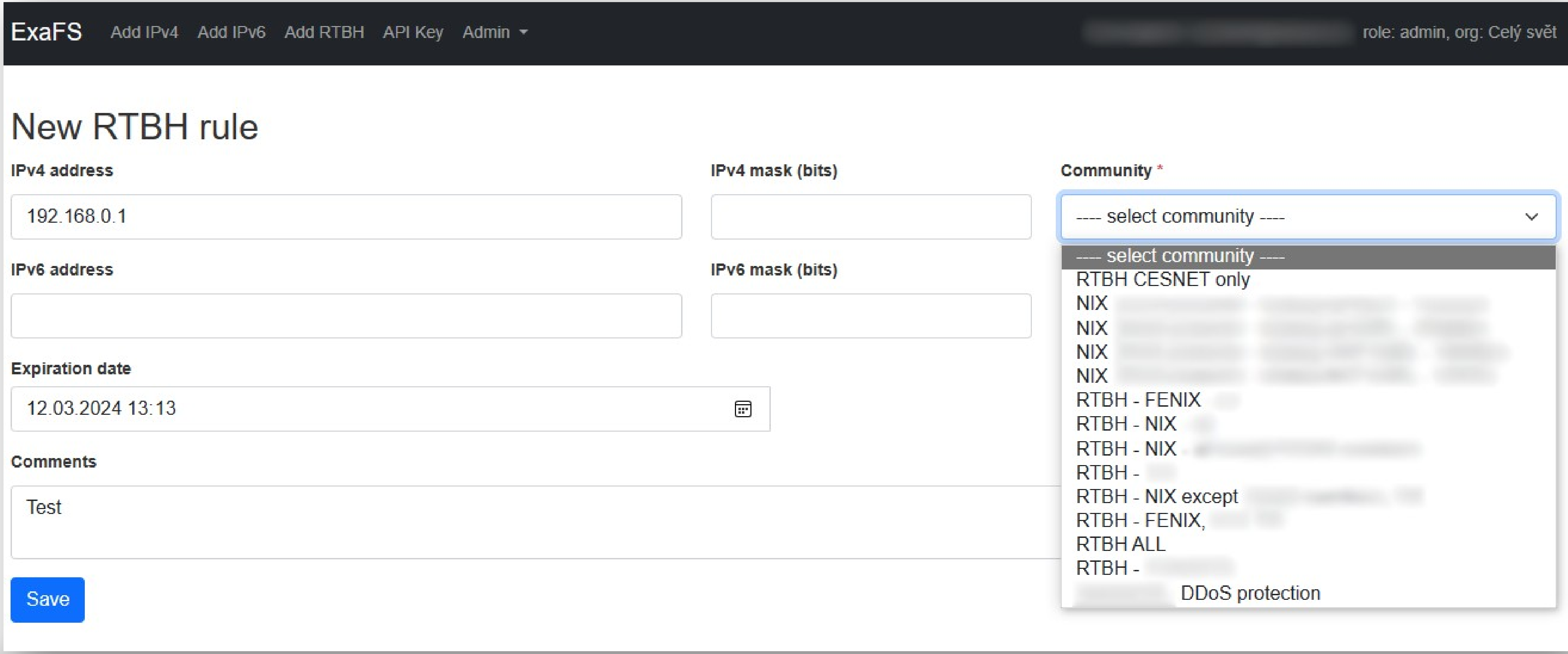
12.03.2024 13:44

ExaFS 0.

Tools

ExaFS UI example

- RTBH rule form



New RTBH rule

IPv4 address: 192.168.0.1

IPv4 mask (bits):

Community *: ---- select community ----

IPv6 address:

IPv6 mask (bits):

Expiration date: 12.03.2024 13:13

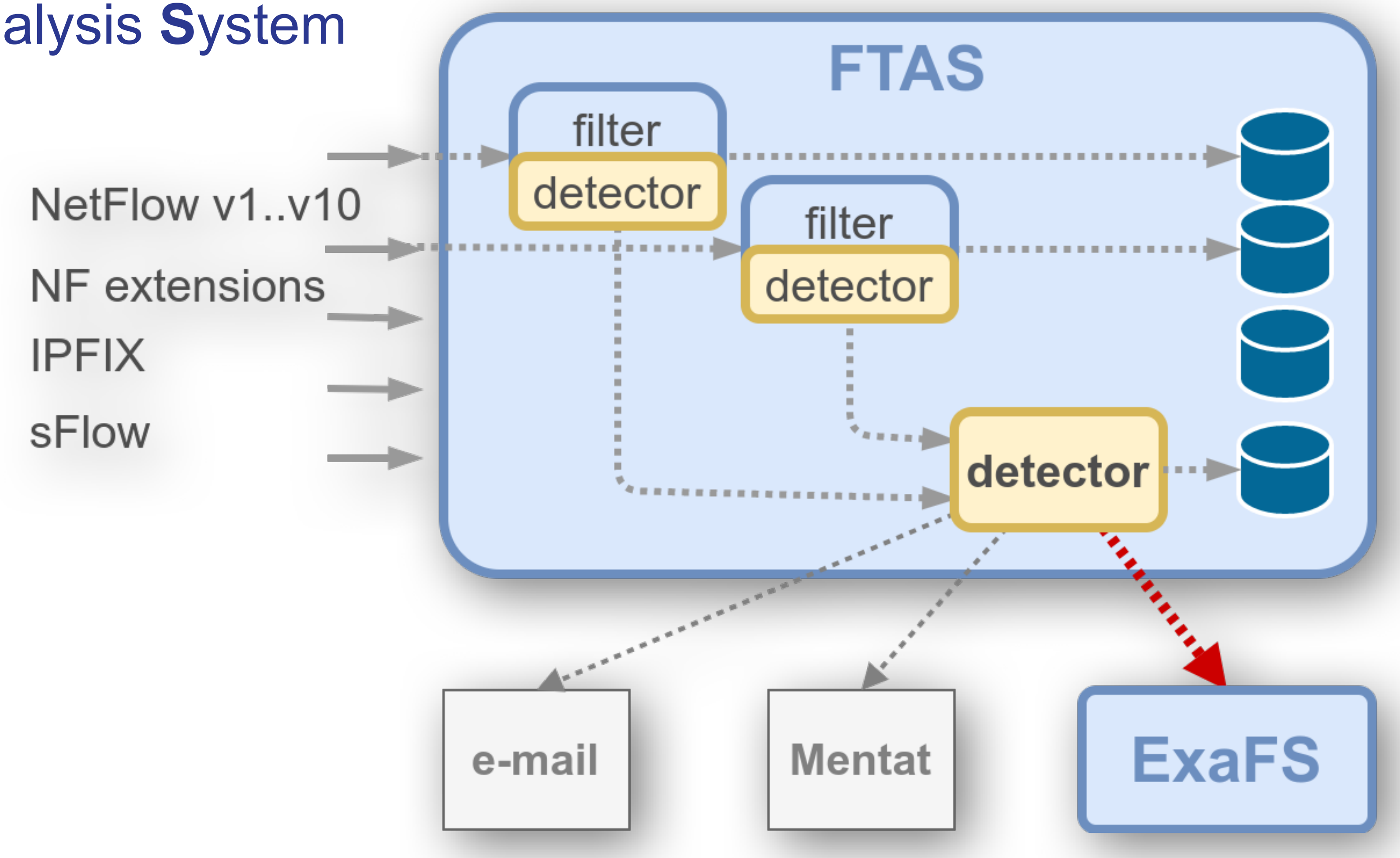
Comments: Test

---- select community ----
RTBH CESNET only
NIX [redacted]
NIX [redacted]
NIX [redacted]
NIX [redacted]
RTBH - FENIX [redacted]
RTBH - NIX [redacted]
RTBH - NIX [redacted]
RTBH - [redacted]
RTBH - NIX except [redacted]
RTBH - FENIX, [redacted]
RTBH ALL
RTBH - [redacted]
[redacted] DDoS protection

Tools

FTAS – Flow-based Traffic Analysis System

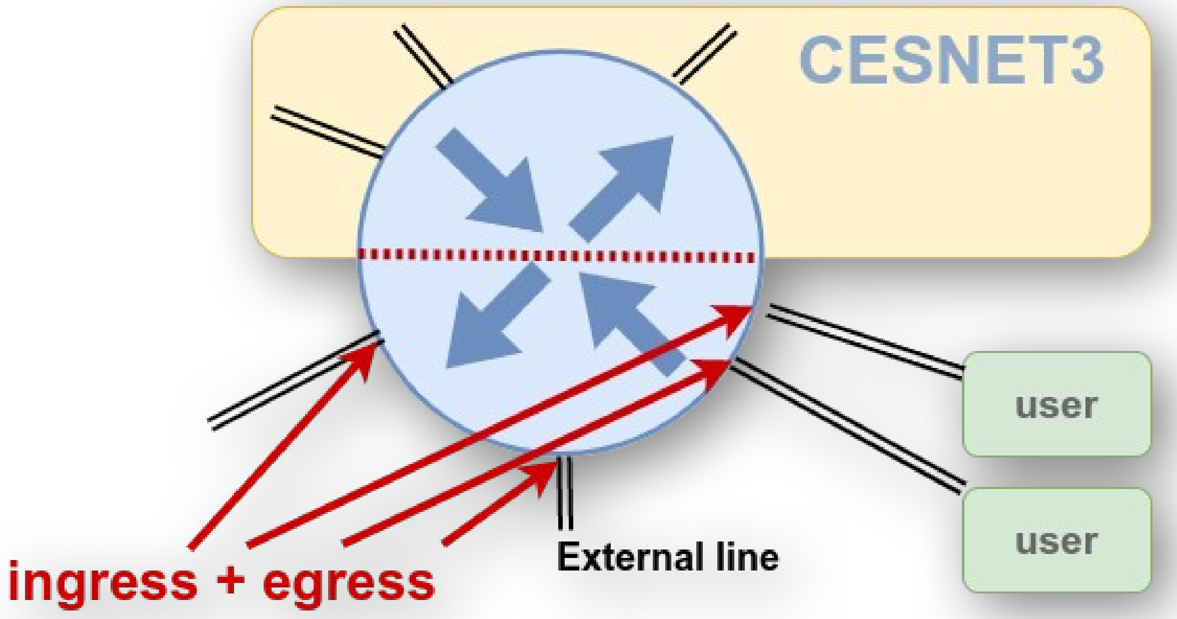
- **flow-based monitoring data processing**, storage, visualization
  - traffic analysis
  - **functionality for detector configurations** (technologically based)
  - extended to **control ExaFS directly** (API)

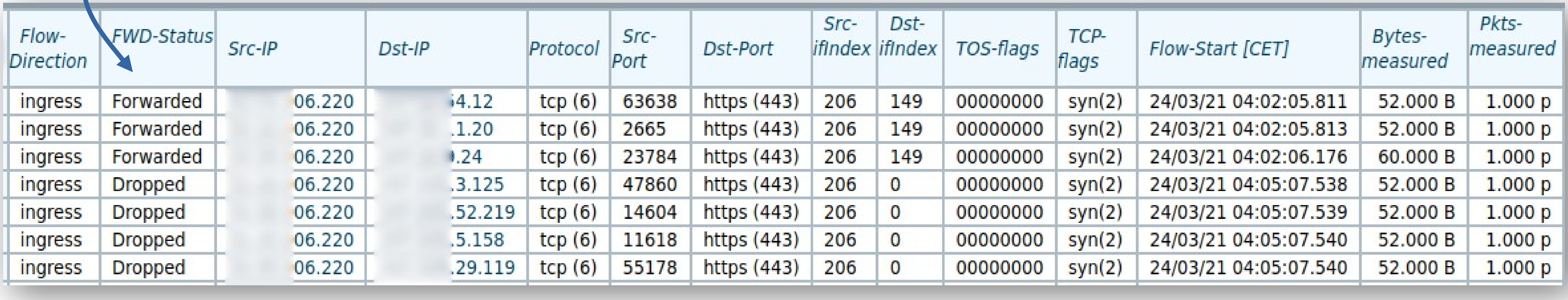


Tools

FTAS - flow information resources setup

- boxes, interfaces, directions
- aggressive NF export
- relatively low sampling
- ingress benefits



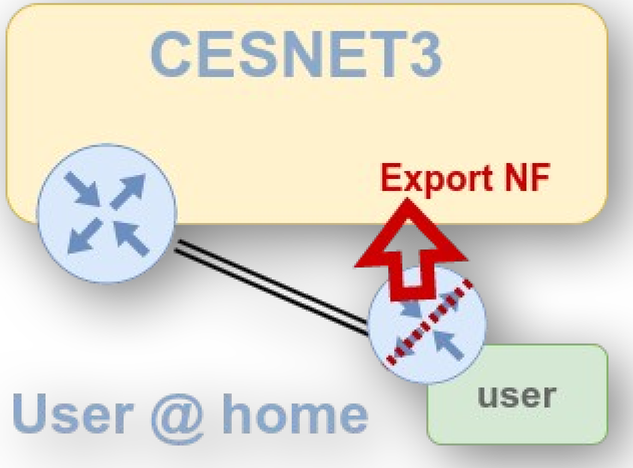


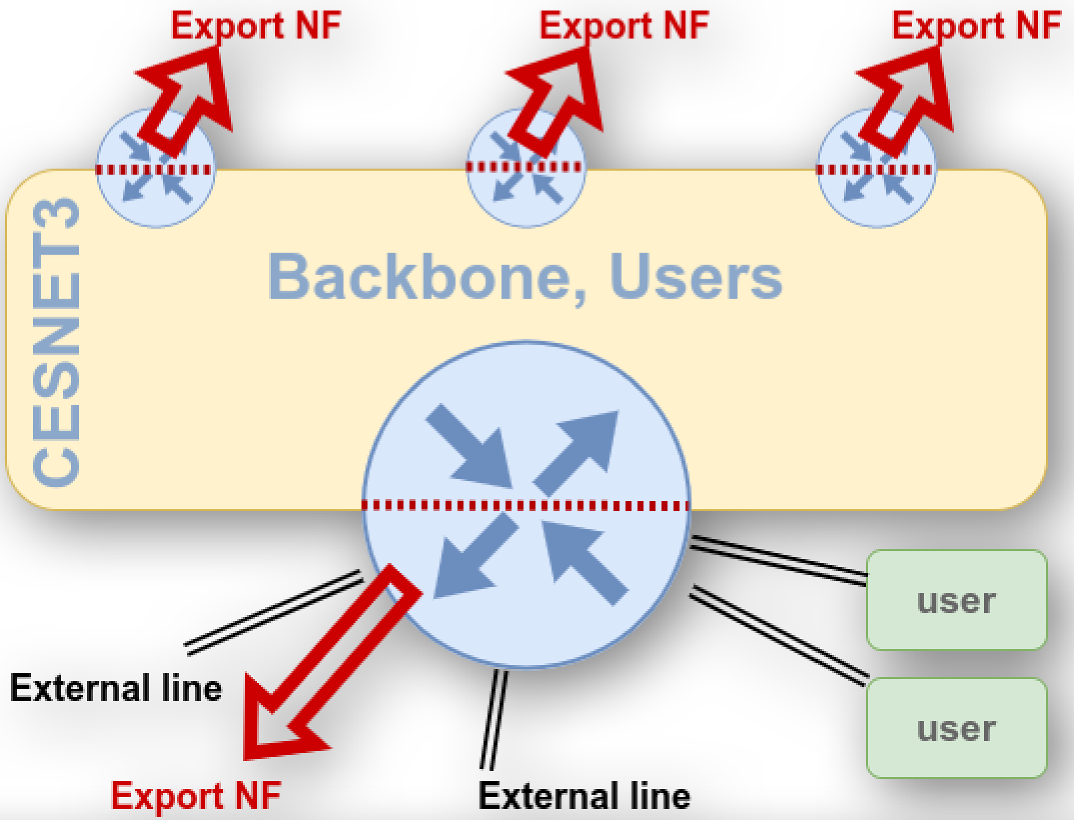
Flow-Direction	FWD-Status	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	TOS-flags	TCP-flags	Flow-Start [CET]	Bytes-measured	Pkts-measured
ingress	Forwarded	[redacted]06.220	[redacted]4.12	tcp (6)	63638	https (443)	206	149	00000000	syn(2)	24/03/21 04:02:05.811	52.000 B	1.000 p
ingress	Forwarded	[redacted]06.220	[redacted].1.20	tcp (6)	2665	https (443)	206	149	00000000	syn(2)	24/03/21 04:02:05.813	52.000 B	1.000 p
ingress	Forwarded	[redacted]06.220	[redacted].24	tcp (6)	23784	https (443)	206	149	00000000	syn(2)	24/03/21 04:02:06.176	60.000 B	1.000 p
ingress	Dropped	[redacted]06.220	[redacted].3.125	tcp (6)	47860	https (443)	206	0	00000000	syn(2)	24/03/21 04:05:07.538	52.000 B	1.000 p
ingress	Dropped	[redacted]06.220	[redacted].52.219	tcp (6)	14604	https (443)	206	0	00000000	syn(2)	24/03/21 04:05:07.539	52.000 B	1.000 p
ingress	Dropped	[redacted]06.220	[redacted].5.158	tcp (6)	11618	https (443)	206	0	00000000	syn(2)	24/03/21 04:05:07.540	52.000 B	1.000 p
ingress	Dropped	[redacted]06.220	[redacted].29.119	tcp (6)	55178	https (443)	206	0	00000000	syn(2)	24/03/21 04:05:07.540	52.000 B	1.000 p

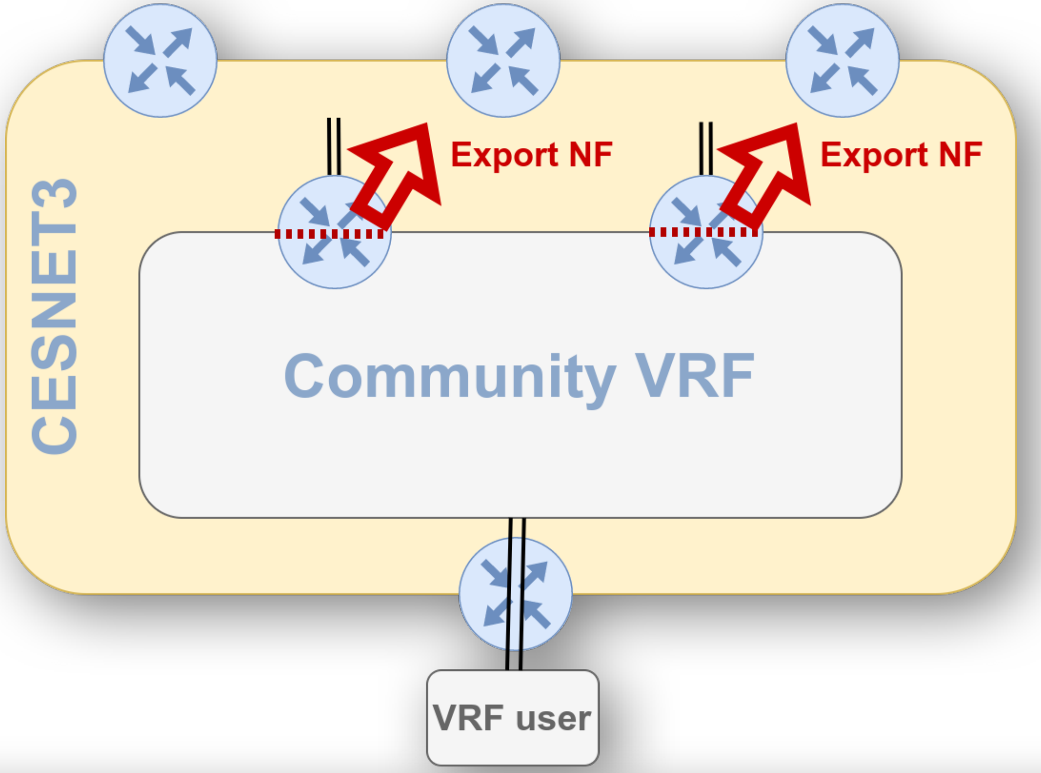
Tools

FTAS - flow information data

- typical relevant flow data sources **for detectors**







Transport Layer Protection Setup

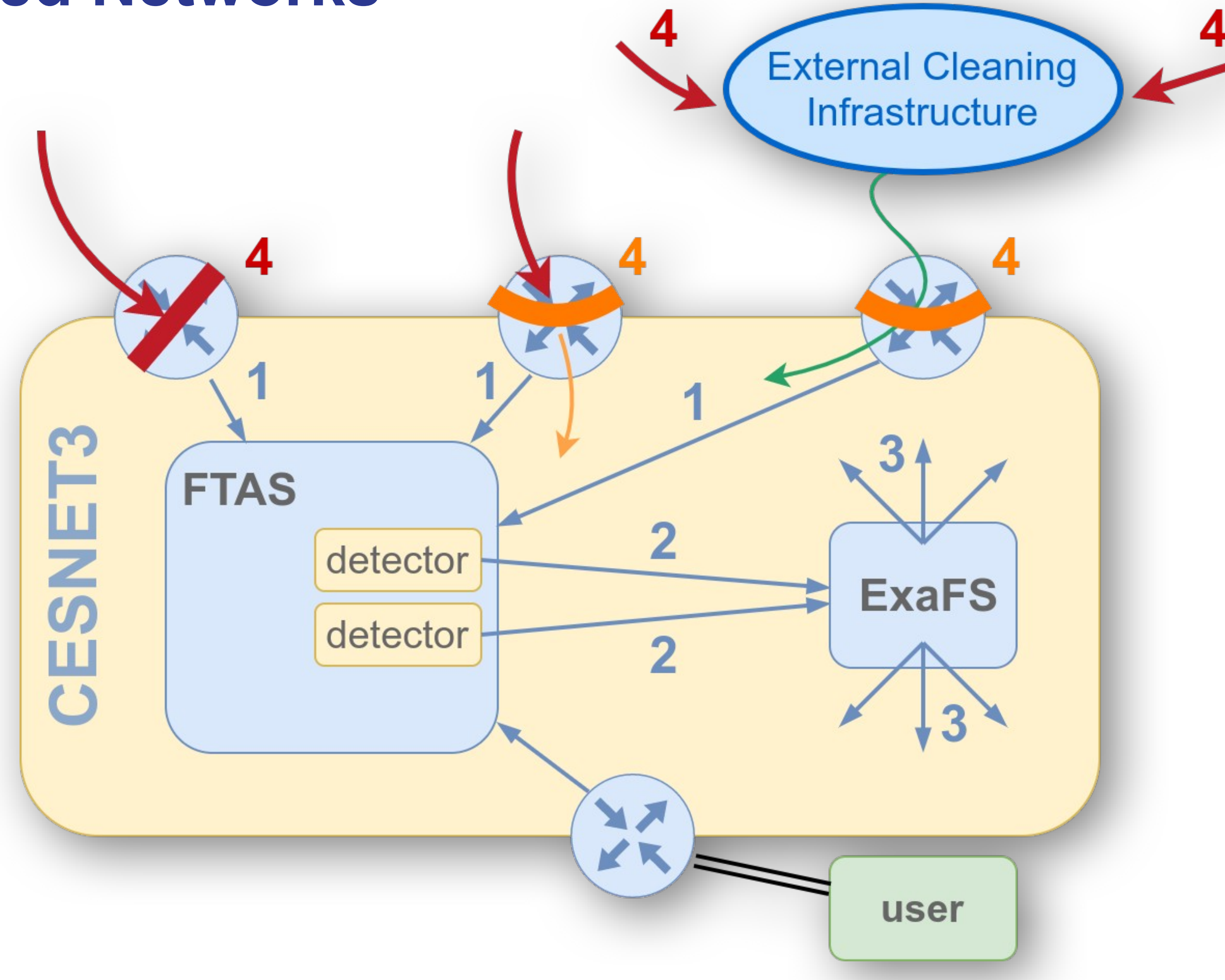
Priorities

- backbone network infrastructure
- user connections
- *external lines*

- NREN resources, users, community support
  - infrastructure attacks
  - various types of platform/service/application attacks
  - discovery (scanning)
  - misuse (mining)

Setup → NREN + All Connected Networks

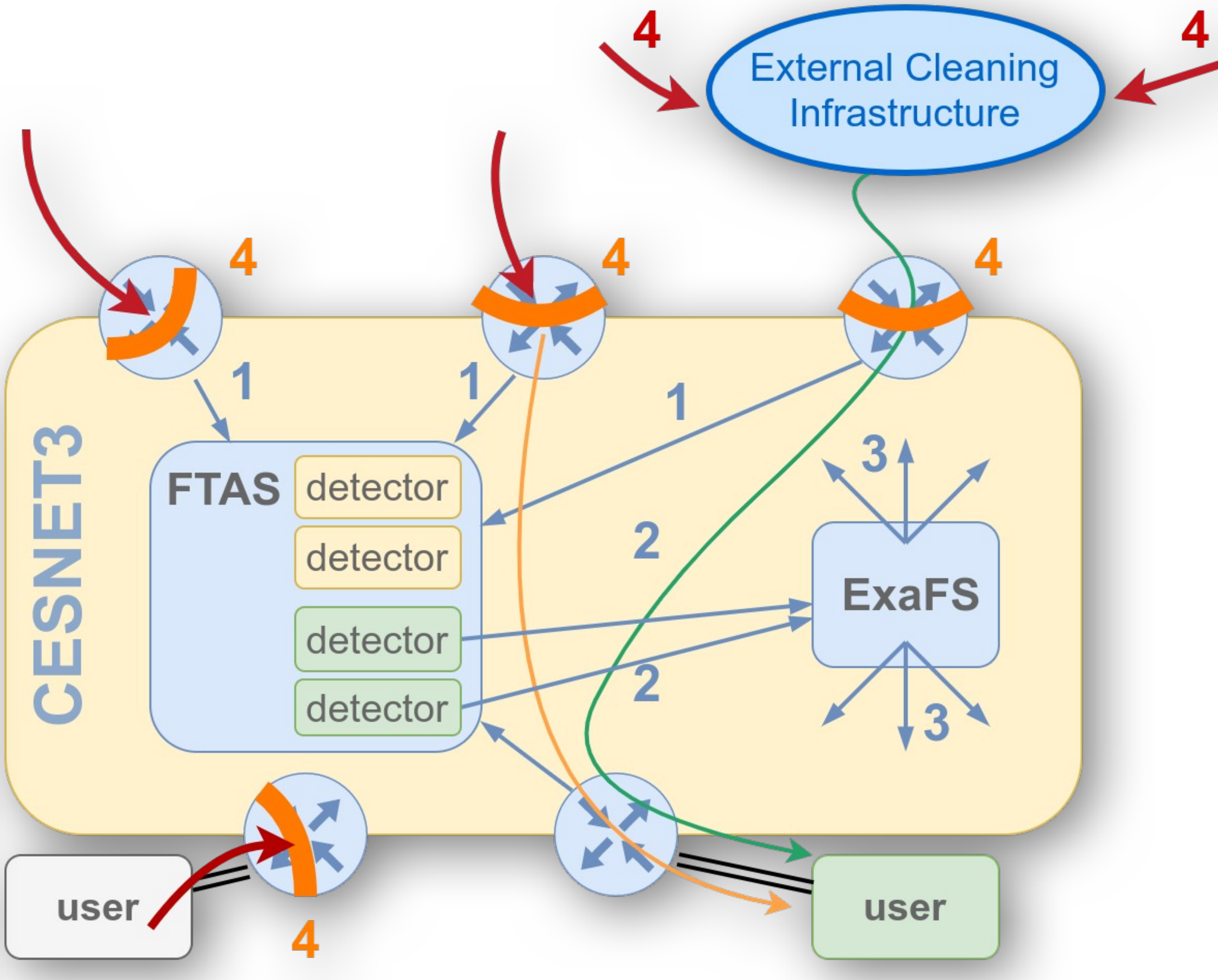
- **first level**
- detectors - limits, types
- incoming traffic
  - techniques
    - **RTBH**
    - **BGP FlowSpec**
    - **external cleaning**
- outgoing traffic
  - semi-automated
    - notifications → CSIRT → IH



Setup → Individual Users

- **second level**
- on demand (infrastructure, application)
  - automated / notifications only
- specific dedicated detectors
- techniques

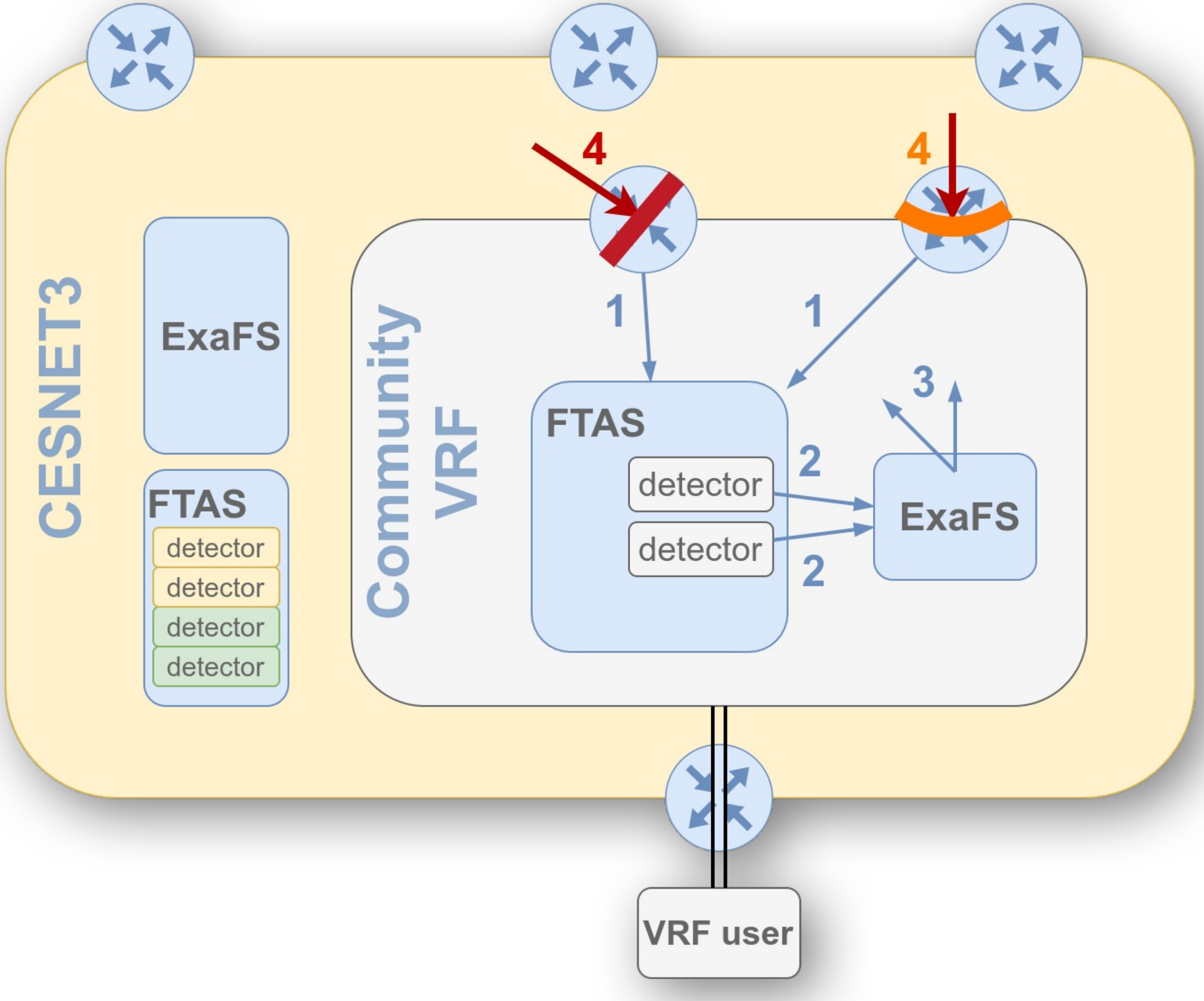
	auto mated	ExaFS self service
RTBH	limitation	dest.
BGP FlowSpec	**yes**	**yes**
external cleaning	**yes**	no
DDoS protector	tbd	tbd



Setup → Community VRF

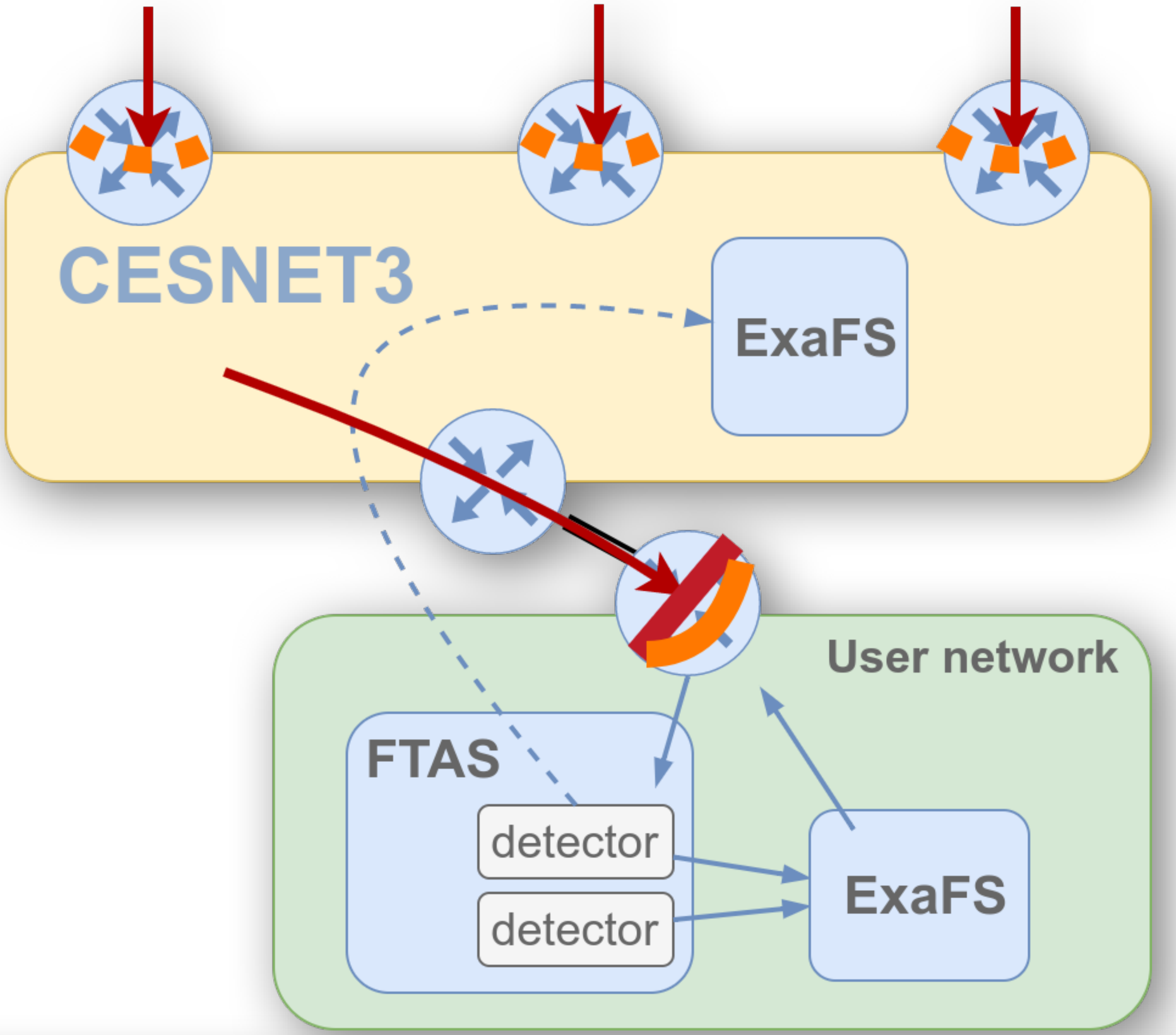
- **second level**
- VRF → users with similar traffic characteristics, behavior, culture, ...
- dedicated ExaFS+FTAS instances (not necessary)
- common + individual detectors
- techniques

	auto mated	ExaFS self service
RTBH	**yes**	dest.
BGP FlowSpec	**yes**	**yes**

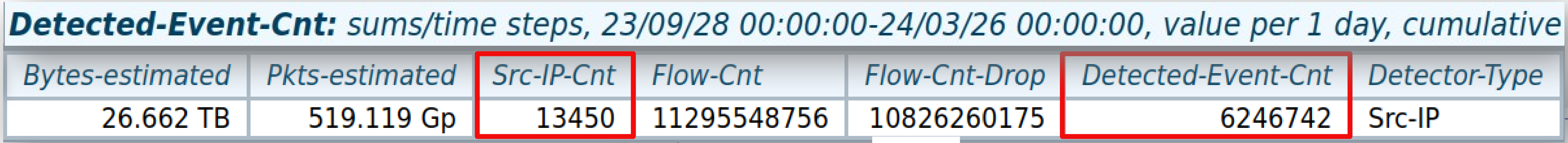


Setup → User in Connected Network

- **second/third level**
- dedicated ExaFS+FTAS
  - generally detectors can be based on any other system that works → network monitoring, on-host monitoring, log management, etc.
- can also use external ExaFS
- techniques
  - **RTBH**
  - **BGP FlowSpec** - if available locally
    - NREN ExaFS instance as alternative



Results Examples

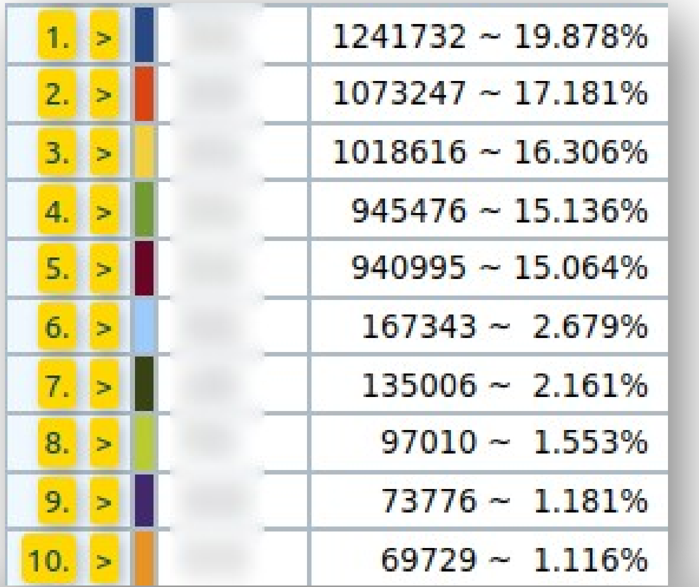


Detected-Event-Cnt: *sums/time steps, 23/09/28 00:00:00-24/03/26 00:00:00, value per 1 day, cumulative*

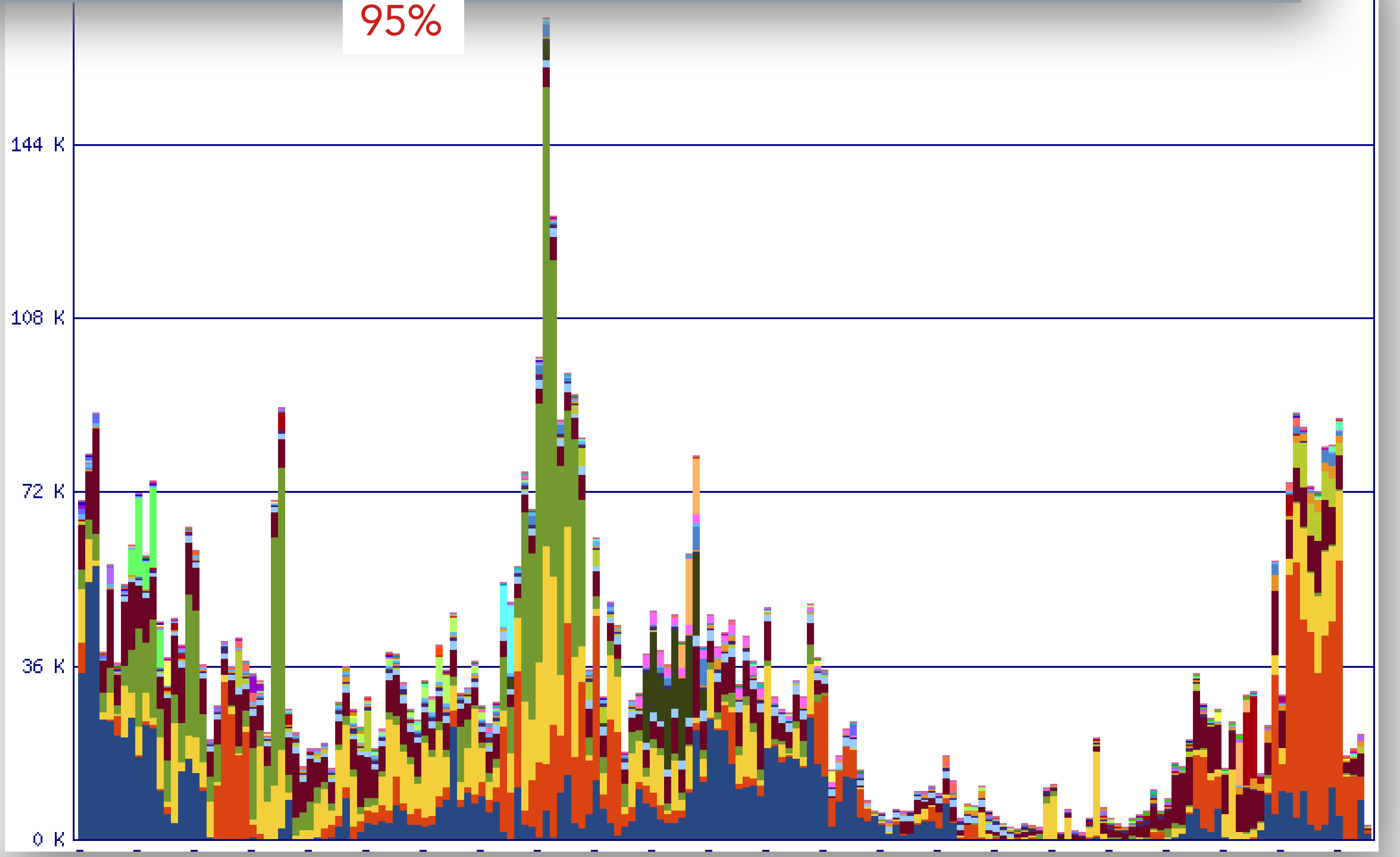
Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
26.662 TB	519.119 Gp	13450	11295548756	10826260175	6246742	Src-IP

95%

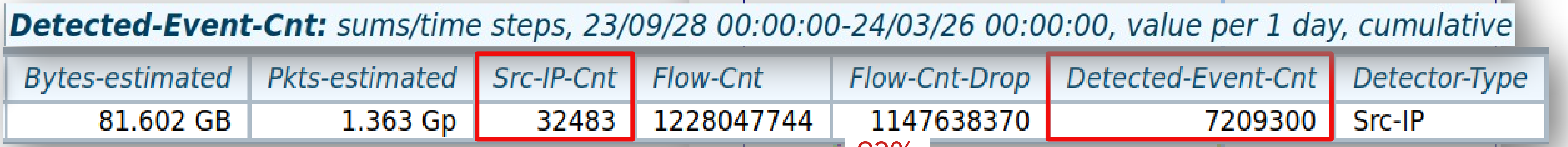
- **first level – NREN & all users**
- event sources
- not all detectors tied with traffic regulation



1.	>	🟦	[redacted]	1241732 ~ 19.878%
2.	>	🟧	[redacted]	1073247 ~ 17.181%
3.	>	🟨	[redacted]	1018616 ~ 16.306%
4.	>	🟩	[redacted]	945476 ~ 15.136%
5.	>	🟥	[redacted]	940995 ~ 15.064%
6.	>	🟦	[redacted]	167343 ~ 2.679%
7.	>	🟩	[redacted]	135006 ~ 2.161%
8.	>	🟩	[redacted]	97010 ~ 1.553%
9.	>	🟪	[redacted]	73776 ~ 1.181%
10.	>	🟧	[redacted]	69729 ~ 1.116%



Results Examples



***Detected-Event-Cnt:** sums/time steps, 23/09/28 00:00:00-24/03/26 00:00:00, value per 1 day, cumulative*

Bytes-estimated	*Pkts-estimated*	*Src-IP-Cnt*	*Flow-Cnt*	*Flow-Cnt-Drop*	*Detected-Event-Cnt*	*Detector-Type*
81.602 GB	1.363 Gp	32483	1228047744	1147638370	7209300	Src-IP

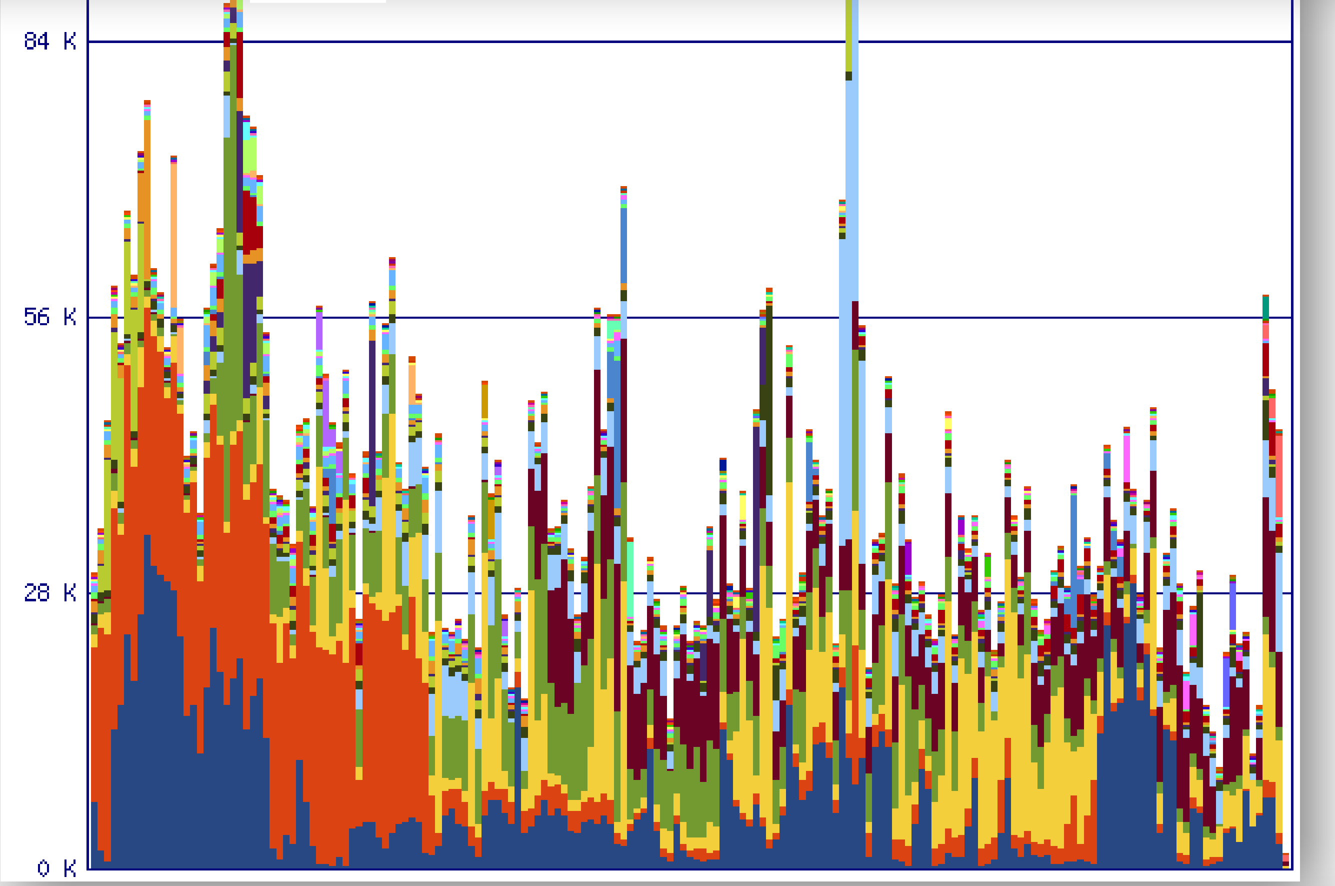
93%

- **second level – Community VRF**
- sources of anomalies

- ~ 2% of addresses

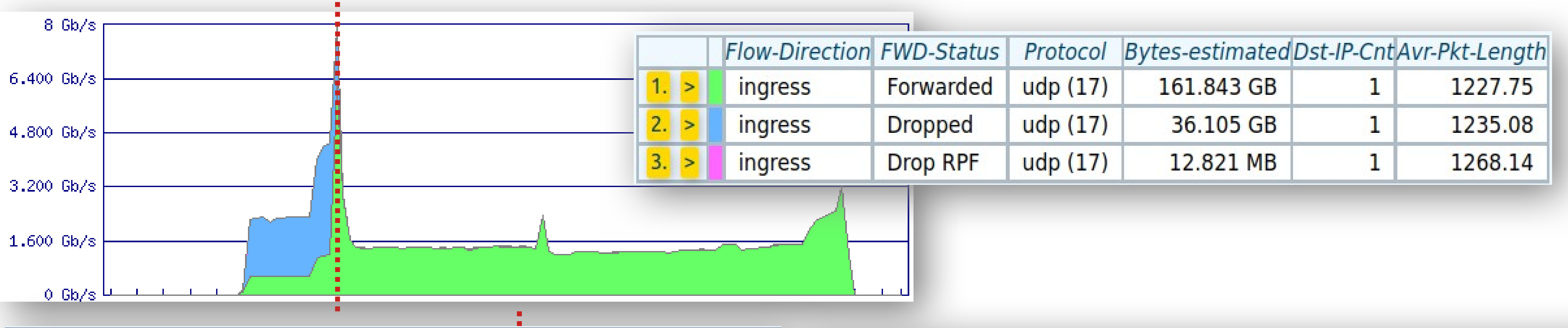
vs.

- higher number of detections and source addresses

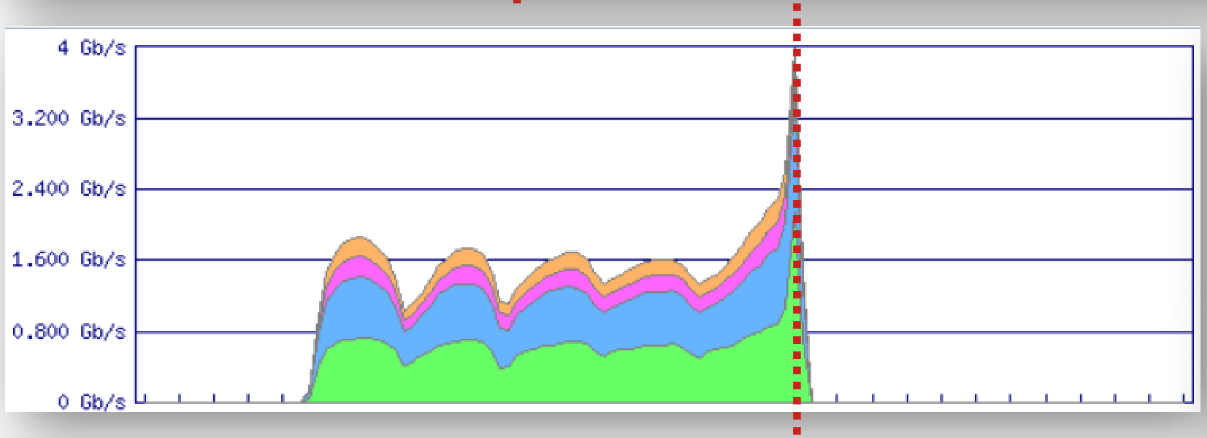


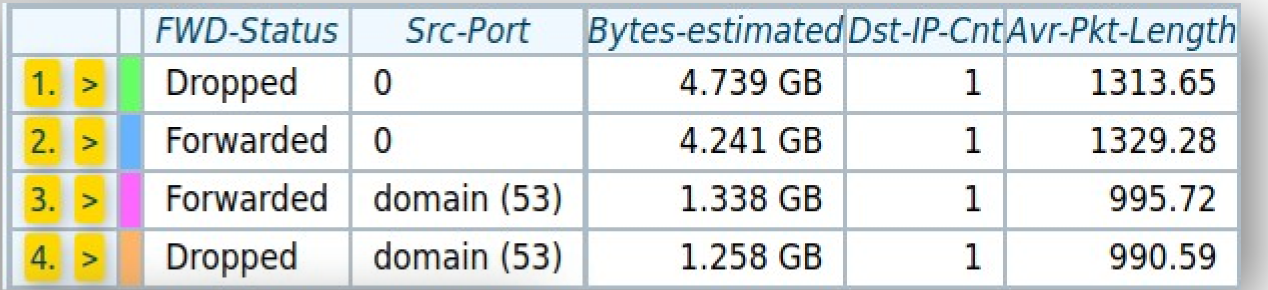
Results Examples

- **~ 5 amplifications/month** in last 6 months
- typically lower rate – examples

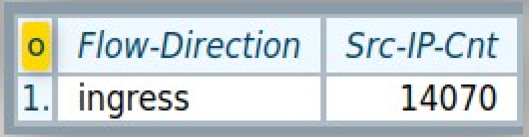


		Flow-Direction	FWD-Status	Protocol	Bytes-estimated	Dst-IP-Cnt	Avr-Pkt-Length
1. >	🟩	ingress	Forwarded	udp (17)	161.843 GB	1	1227.75
2. >	🟦	ingress	Dropped	udp (17)	36.105 GB	1	1235.08
3. >	🟪	ingress	Drop RPF	udp (17)	12.821 MB	1	1268.14





		FWD-Status	Src-Port	Bytes-estimated	Dst-IP-Cnt	Avr-Pkt-Length
1. >	🟩	Dropped	0	4.739 GB	1	1313.65
2. >	🟦	Forwarded	0	4.241 GB	1	1329.28
3. >	🟪	Forwarded	domain (53)	1.338 GB	1	995.72
4. >	🟧	Dropped	domain (53)	1.258 GB	1	990.59



o	Flow-Direction	Src-IP-Cnt
1.	ingress	14070

False Positives

- unpredicted vs. predicted ?

Notices / Lessons learned

- flow-based detection → clearly determines range of effective use *(observing packets not application data...)*
- communication with users → to explain over and over again → expectations vs. reality, their mindset evolution
- it’s team work with lot of courage necessary – many thanks to great colleagues !!!
- **this is a prevention → taking care of stable infrastructure services and data delivery** → focusing whole system & user community ..hard to transpose to managers’ perspective: ”How many attacks against our institution have you mitigated ?”

GÉANT

Modular transport layer solution for semi/automated protection of infrastructure, communities and users in CESNET3 network

Thank You !!!

Any questions?

Security
.Days

Co-funded by
the European Union