cesnet

Monitoring a měření

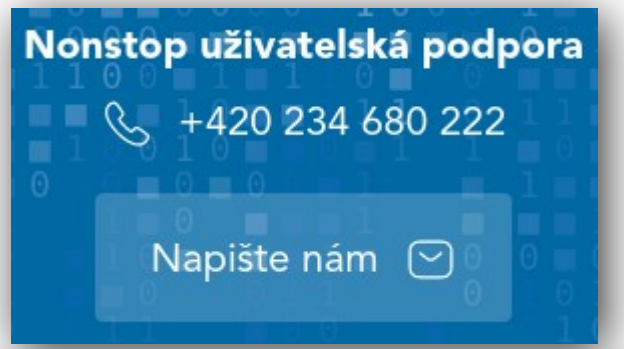
Tomáš Košňar
CESNET

CESNET DAY - ČZU
15. 5. 2024

Základní dohled

NOC / HelpDesk / Service Desk

- **support@cesnet.cz**
- **www/cesnet.cz → kontakty**
- 24x7
- základní úroveň dohledu / podpory
- rozcestník k vyšším úrovním podpory
- služba pohotovosti síťového specialisty 24x7



Východisko

..o čem nemám informace, to nejsem schopen řídit ani gramotně spravovat..

Základní okruhy otázek

- v jakém stavu je infrastruktura ?
- jaké datové přenosy byly infrastrukturou uskutečněny, kudy data tekla ?
- kdo/co stojí za konkrétním datový přenosem ?
- umíme analyzovat/detekovat provozní anomálie/útoky ?

Členění problematiky

- monitoring infrastruktury
- monitoring provozu

Smysl, potřebnost

- **každá síť, bez ohledu na to kam je připojena, by měla mít souvislý monitoring alespoň základních metrik popisujících stav, chování a využití..**

- síťové prvky, významné zdroje (servery, virtualizační platformy, specifická zařízení…)

- up/down state, packet rates, bit rates, discards, errors, charakteristiky připojení na fyzickou vrstvu apod. na rozhraních, ..CPU na prvcích, teploty, alokace paměti apod.

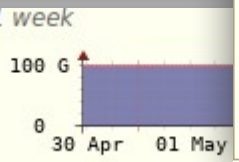
- ++ pokud to umí zahlásit překročení nastavených limitů (zátěž, chybovost,..), změny stavů ..

cesnet

Monitoring infrastruktury

Speed *[bps]*

technical	max=100.0G
input (admin.)	max=100.0G
output (admin.)	max=100.0G

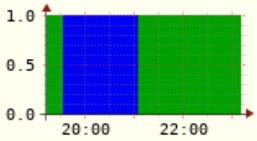


Measured interfaces *2024/05/08 19:10:04 ... 2024/05/08 23:10:04*

Found
max=1

Admin. up
max=1

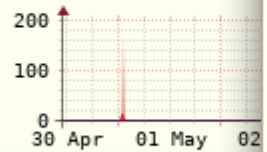
Operating
max=1



Errors *[pps]*

Input errors
min=0.000
max=164.175
avr=128.240m

Output errors
min=0.000
max=0.000



Discards *[pps]*

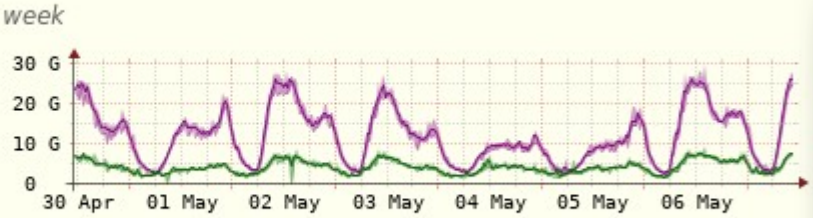
Input discards
min=0.000
max=0.000
avr=0.000

Output discards
min=0.000
max=0.000

Bit rates *[bps]*

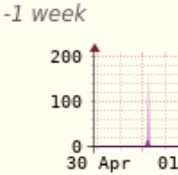
Input
min=2.265G
max=29.492G
avr=12.150G

Output
min=22.366M
max=9.069G
avr=4.148G



Ethernet errors *[fps]*

alignment errors	min=0.000 max=0.000 avr=0.000
checksum errors	min=0.000 max=0.000 avr=0.000
frames too long	min=0.000 max=168.195 avr=128.259m
SQE test errors	min=0.000 max=0.000 avr=0.000
internal MAC transmit errors	min=0.000 max=0.000 avr=0.000
internal MAC receive errors	min=0.000 max=0.000 avr=0.000
carrier sense errors	min=0.000 max=0.000 avr=0.000



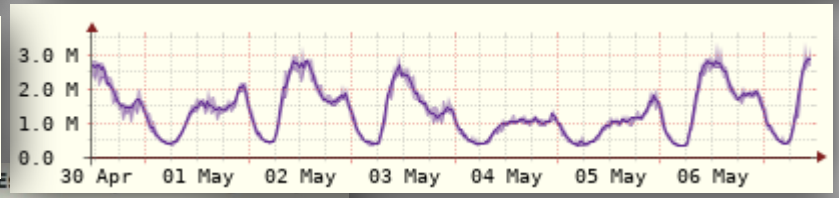
Input/Output traffic ratio *[%]*

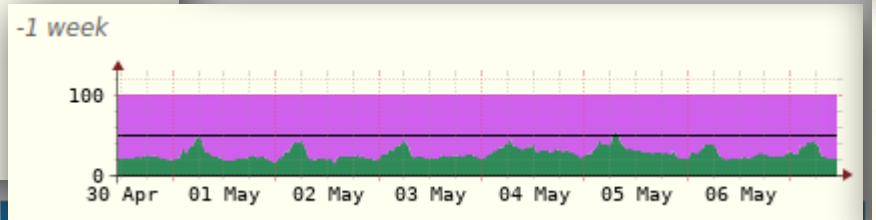
Input
min=45.535
max=85.409
avr=71.882

Output
min=14.591
max=54.465
avr=28.118

Packet rates per class - Input

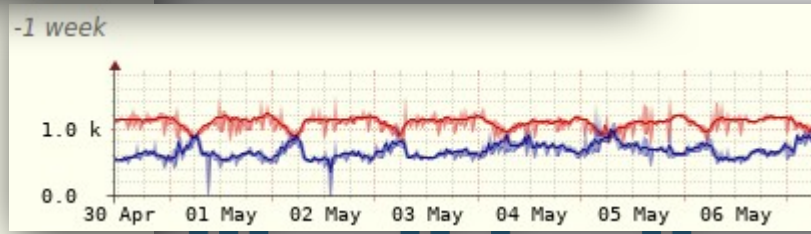
Unicasts	min=334.171k max=3.362M avr=1.347M
Multicasts	min=15.872 max=86.598 avr=48.550
Broadcasts	min=45.822 max=281.797 avr=114.346





Input
min=765.227
max=1.512k
avr=1.106k

Output
min=1.827
max=1.380k

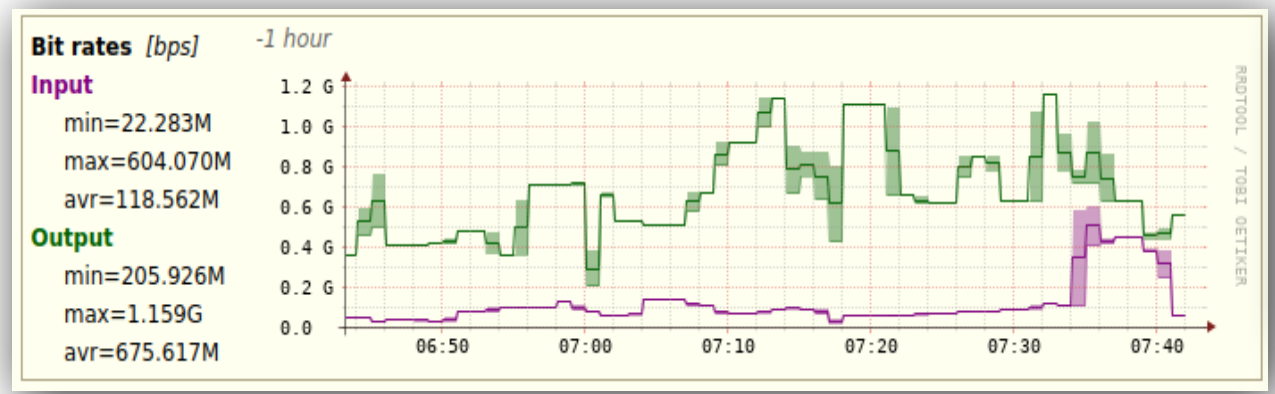


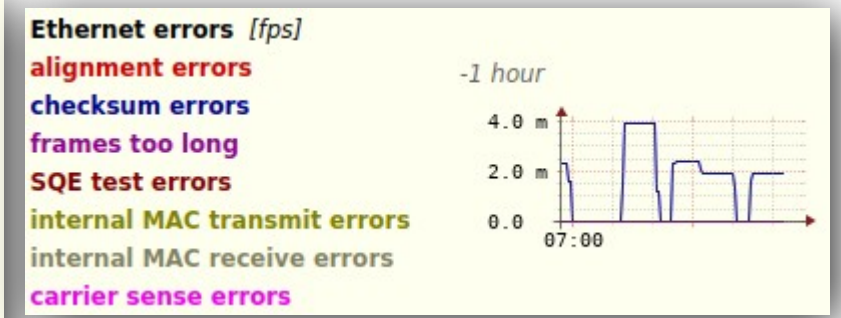
Sběr dat, nástroje

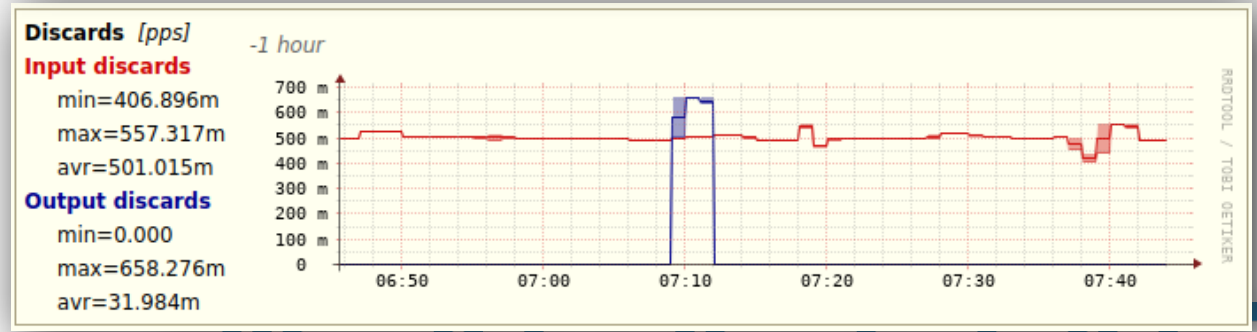
- sběr dat
  - SNMP
  - telemetrie
- zpracování - známé/popsané workflow i na open source nástrojích
  - telegraf, influx+grafana, prometheus
  - CACTi, MRTG, MUNIN, LibreNMS, ...
  - lze implementovat např. i jako metriky v zabbixu / nagios / icinga

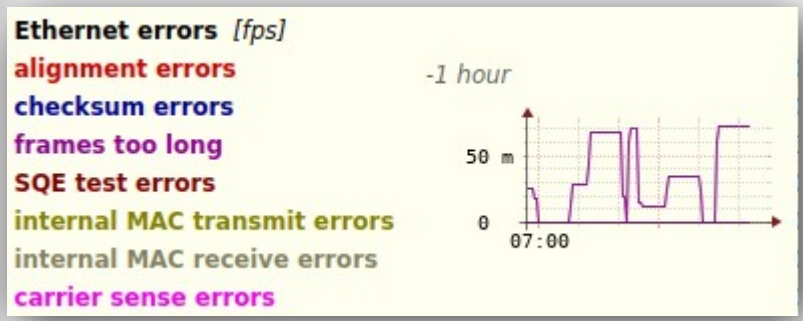
Interpretace dat ..bez ohledu na použitý nástroj

- správná interpretace ← znalost způsobu měření, znalost významu



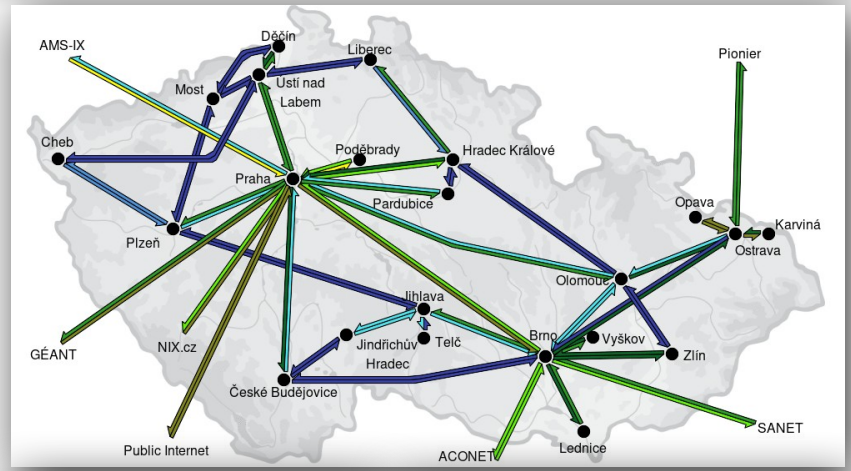


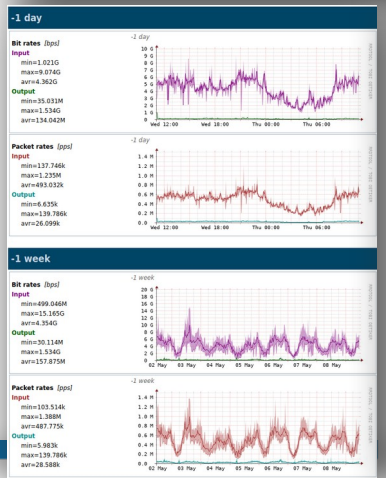


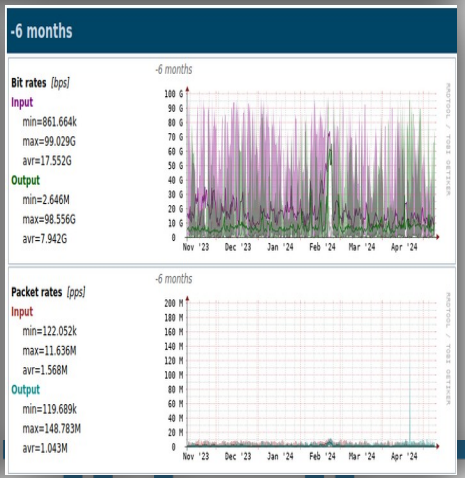


systém G3

- vlastní nástroj, historicky vyvinut pro potřeby monitoringu páteřní sítě (přesnější/detailnější informace oproti tehdy dostupným)
- může být nasazen i v lokálních sítích
- periodický sběr dat z prvků infrastruktury *(dominantně SNMP, minimalistická konfigurace)*
- seskupení naměřených dat ze zařízení → logická struktura zařízení, uložení dat
- přístup k datům
  - interaktivní UI - vyhledávání objektů + vizualizace objektů (vč. agregované)
  - vizualizace událostí
  - notifikace událostí



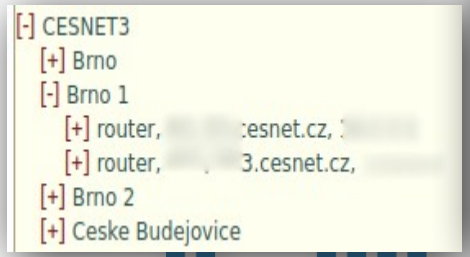


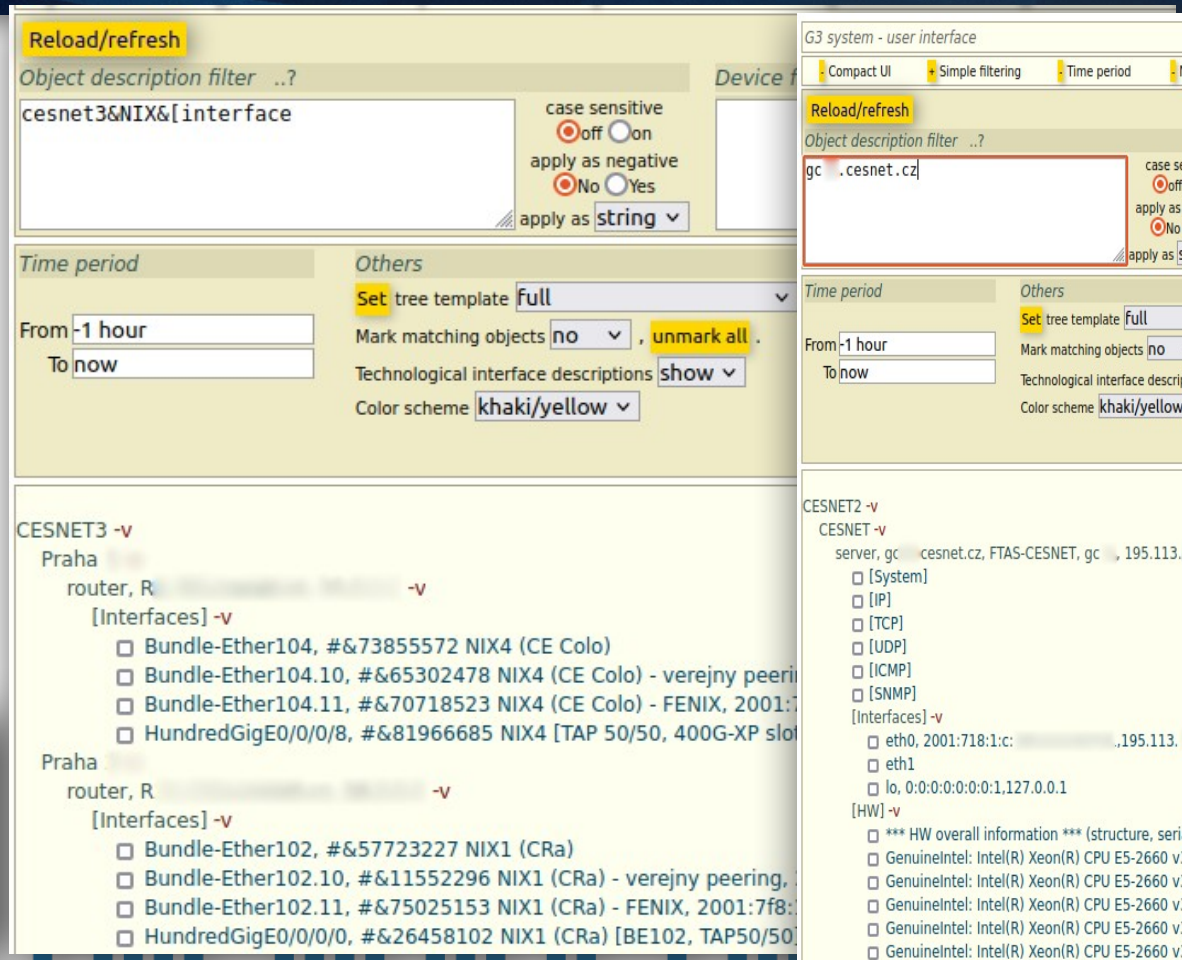


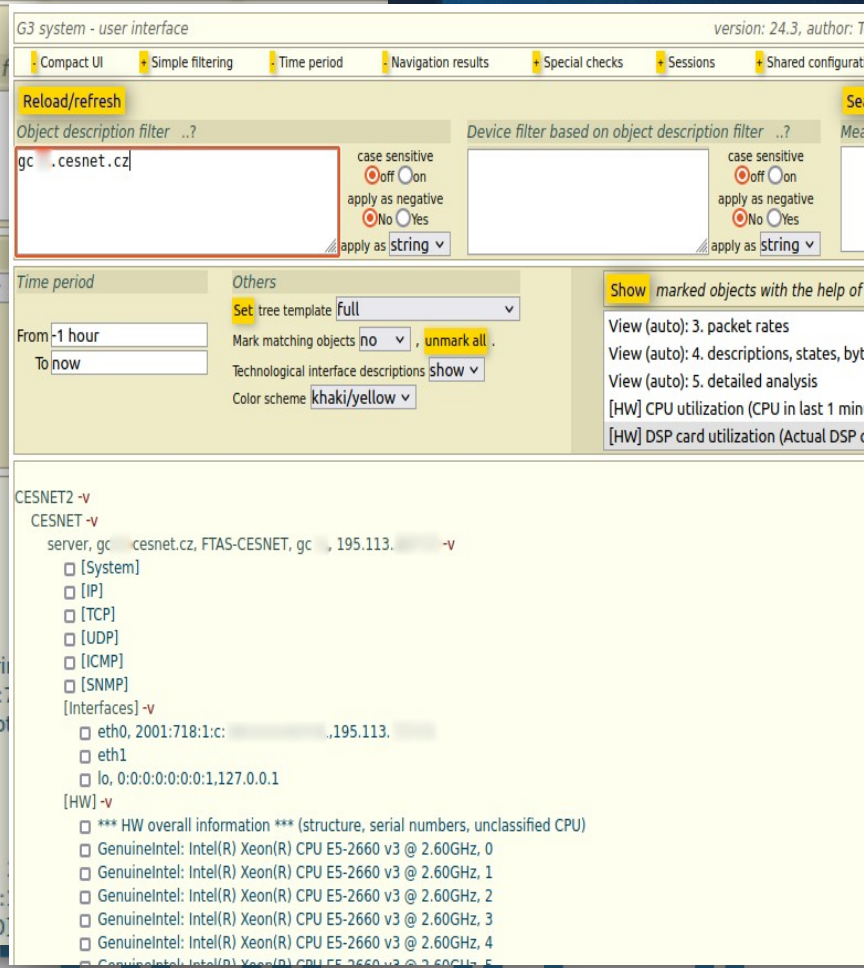
Monitoring infrastruktury

systém G3

- ukázka UI
- vyhledání
- struktura objektů
- expand & collapse





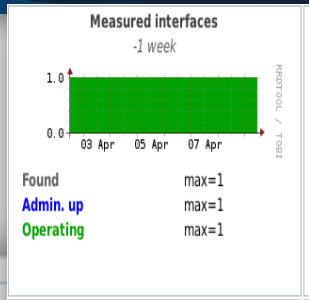


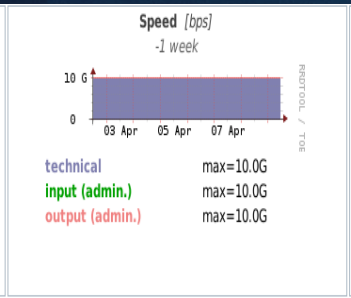
Monitoring infrastruktury

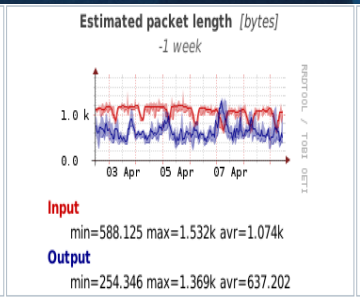
systém G3

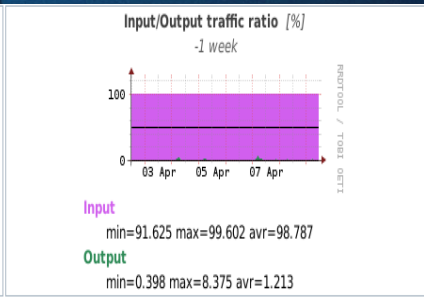
- ukázka UI - vizualizace

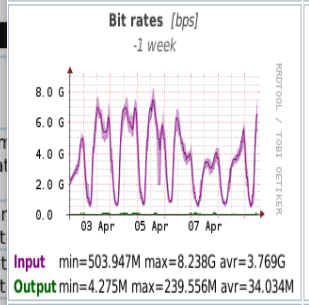
Parameters	
type	ethernetCsmacd
interface description	TenGigE0/1/0/9, [redacted]
IP address	2001:718:0[redacted] fe80:0:0:0:8a1d:fcff:fefb:597f 195.113[redacted]
IPv6 address parameters [1]	2001:718:0[redacted], inaccessible, manual, n fe80:0:0:0:8[redacted] preferred, stateful, stat fe80:0:0:0:8[redacted] stateless, unicast
IPv6 address parameters [2]	2001:718:0[redacted], unicast, preferred, mar fe80:0:0:0:8[redacted] unicast, preferred, stat
IPv6 address parameters [3]	2001:718:0[redacted], unicast, preferred, stat fe80:0:0:0:8[redacted] unicast, preferred, stat
IPv6 address parameters [4]	2001:718:0[redacted], unicast, preferred, mar fe80:0:0:0:8[redacted] unicast, preferred, stat
IPv6 address parameters [5]	2001:718:0[redacted], unicast, preferred, stat fe80:0:0:0:8[redacted] unicast, preferred, stat
IPv6 address parameters [6]	2001:718:0[redacted], unicast, preferred, mar fe80:0:0:0:8[redacted] unicast, preferred, stat
IP network	2001:718:0[redacted] fe80:0:0:0:8a1d:fcff:fefb:597f/128 195.113[redacted]/255.255.255.254
phys. addr.	88:1d:fc:fb:59:7f
MTU	9216
IPv6 effective MTU	9202
IPv6 Physical Address	88:1d:fc:fb:59:7f
SNMP index	162

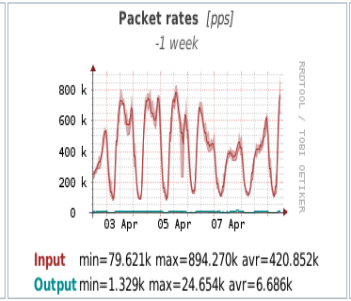


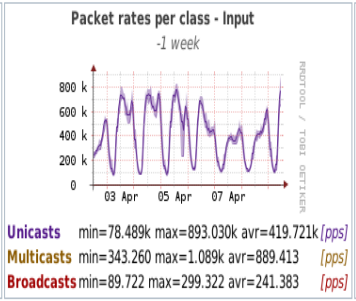


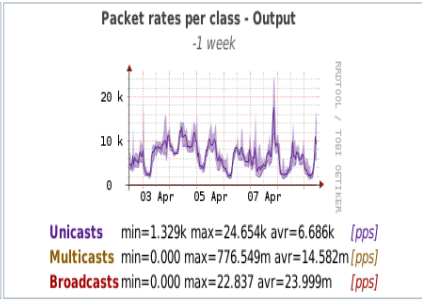


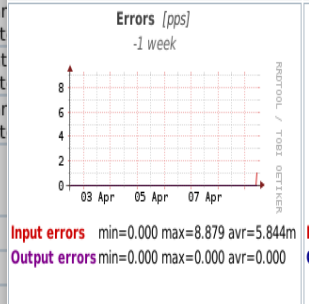


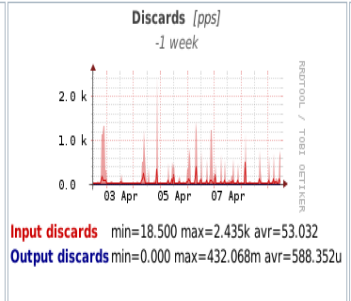


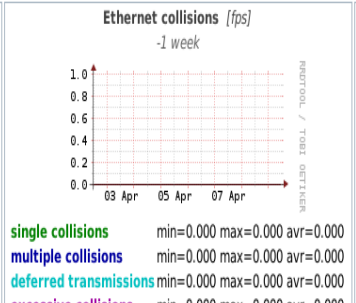


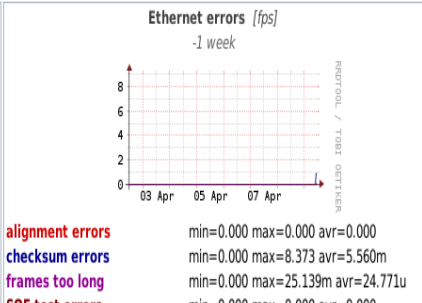












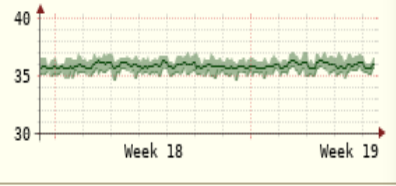
systém G3

- ukázka UI - vizualizace

0/0-Hot Swap Fixed CS, sensor, Board Current Sensor, N/A

-12 day

Sensor with thresholds		
power/level	min=-nan max=-nan avr=-nan	[dBm]
true state	min=-nan max=-nan avr=-nan	[1]
electric current	min=34.604 max=37.133 avr=35.891	[amperes]

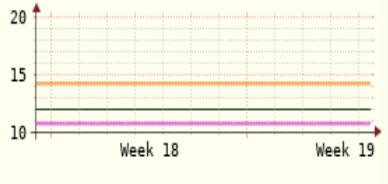


View (auto): 5. detailed anal

0/0-Hot Swap Fixed VS, sensor, Board Voltage Sensor, N/A

Sensor with thresholds		
power/level	min=-nan max=-nan avr=-nan	[dBm]
true state	min=-nan max=-nan avr=-nan	[1]
electric potential DC	min=12.000 max=12.000 avr=12.000	[volts]
greater or equal critical threshold	min=14.4 max=14.4	
greater or equal major threshold	min=14.3 max=14.3	
greater or equal minor threshold	min=14.3 max=14.3	
less or equal critical threshold	min=10.8 max=10.8	
less or equal major threshold	min=10.9 max=10.9	
less or equal minor threshold	min=10.9 max=10.9	

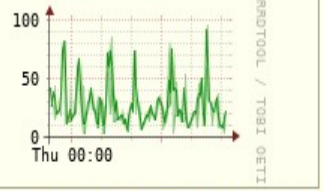
-12 day



GenuineIntel: Intel(R) Xeon(R) Gold 6242R CPU @ 3.10GHz, 0

-12 hour

CPU utilization		
CPU current load	min=3.000 max=95.000 avr=28.598	[%]

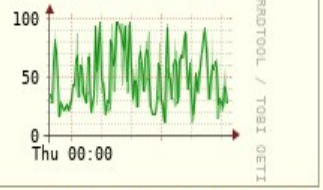


View (auto): 5. detailed analysis

GenuineIntel: Intel(R) Xeon(R) Gold 6242R CPU @ 3.10GHz, 1

-12 hour

CPU utilization		
CPU current load	min=11.000 max=97.000 avr=51.238	[%]

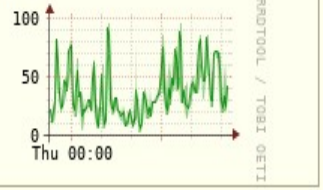


View (auto): 5. detailed analysis

GenuineIntel: Intel(R) Xeon(R) Gold 6242R CPU @ 3.10GHz, 2

-12 hour

CPU utilization		
CPU current load	min=4.000 max=96.000 avr=37.463	[%]



View (auto): 5. detailed analysis

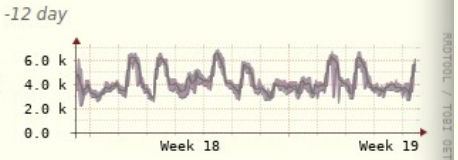
systém G3

- ukázka UI - vizualizace

IP input traffic

Received datagrams
min=2.237k
max=6.933k
avr=4.227k [dtgm/s]

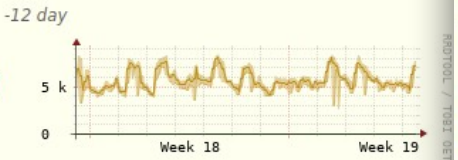
Locally delivered datagrams
min=2.237k
max=6.933k
avr=4.227k [dtgm/s]



IP output traffic

Forwarded datagrams
min=0.000
max=0.000
avr=0.000 [dtgm/s]

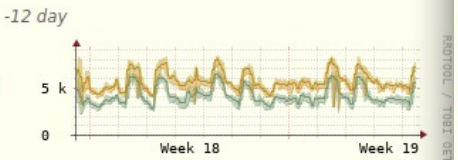
Local output requests
min=2.742k
max=8.517k
avr=5.760k [dtgm/s]



IP local traffic

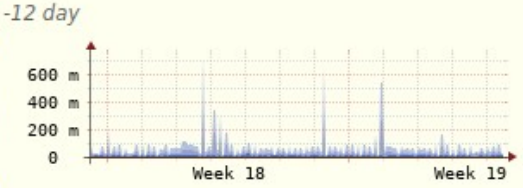
Locally delivered datagrams
min=2.237k
max=6.933k
avr=4.227k [dtgm/s]

Local output requests
min=2.742k
max=8.517k
avr=5.760k [dtgm/s]



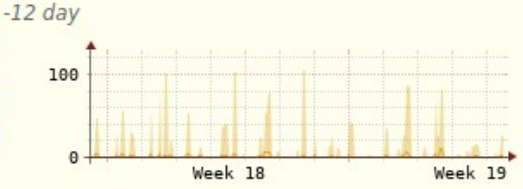
IP reassembling and framentation

Fragments needed to be reassembled	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Reassembled OK	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Reassembly failures	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Fragmented OK	min=0.000 max=365.486m avr=4.055m	[dtgm/s]
Fragments created	min=0.000 max=730.971m avr=8.110m	[fragment/s]
Discarded - "don't fragment flag set" while fragmentation needed	min=0.000 max=0.000 avr=0.000	[dtgm/s]



IP problems

Input header errors	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Input destination address error	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Input unknown/unsupported protocol (locally addressed)	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Input discards	min=0.000 max=0.000 avr=0.000	[dtgm/s]
Output discards	min=0.000 max=103.853 avr=750.313m	[dtgm/s]
No output route	min=0.000 max=0.000 avr=0.000	[dtgm/s]



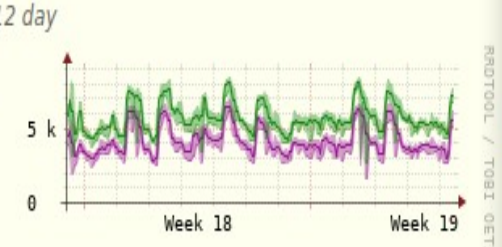
systém G3

- ukázka UI - vizualizace

UDP traffic

Input datagrams
min=1.599k
max=6.921k
avr=4.220k [dtgm/s]

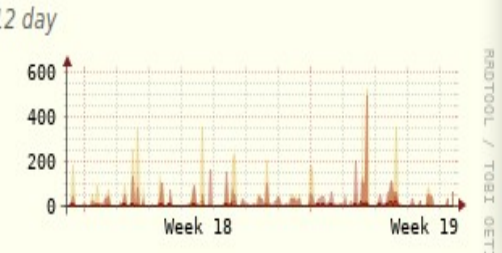
Output datagrams
min=2.666k
max=8.514k
avr=5.759k [dtgm/s]



UDP problems

Invalid port
min=0.000
max=558.118
avr=2.340 [dtgm/s]

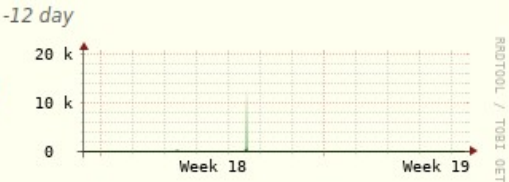
Input errors
min=0.000



TCP traffic

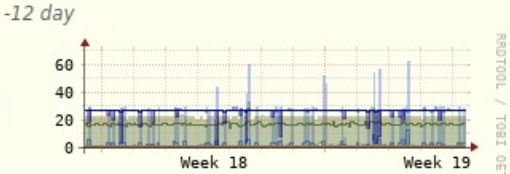
Input segments
min=68.660m
max=1.072k
avr=1.311 [segments/s]

Output segments
min=171.650m
max=13.155k
avr=4.575 [segments/s]



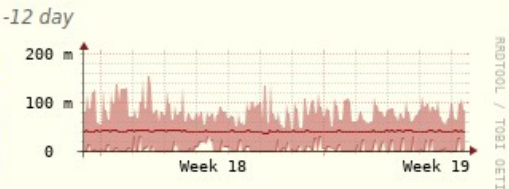
TCP connections and connection states

CLOSED to SYN-SENT	min=0.000 max=62.000 avr=2.349	[connections]
LISTEN to SYN-RCVD state	min=0.000 max=33.000 avr=16.820	[connections]
SYN-SENT or SYN-RCVD to CLOSED plus SYN-RCVD to LISTEN	min=0.000 max=1.000 avr=1.511m	[connections]
ESTABLISHED or CLOSE-WAIT to CLOSED	min=0.000 max=3.000 avr=1.534	[connections]
TCP connections ESTABLISHED or CLOSE-WAIT	min=2.000 max=30.000 avr=26.920	[connections]



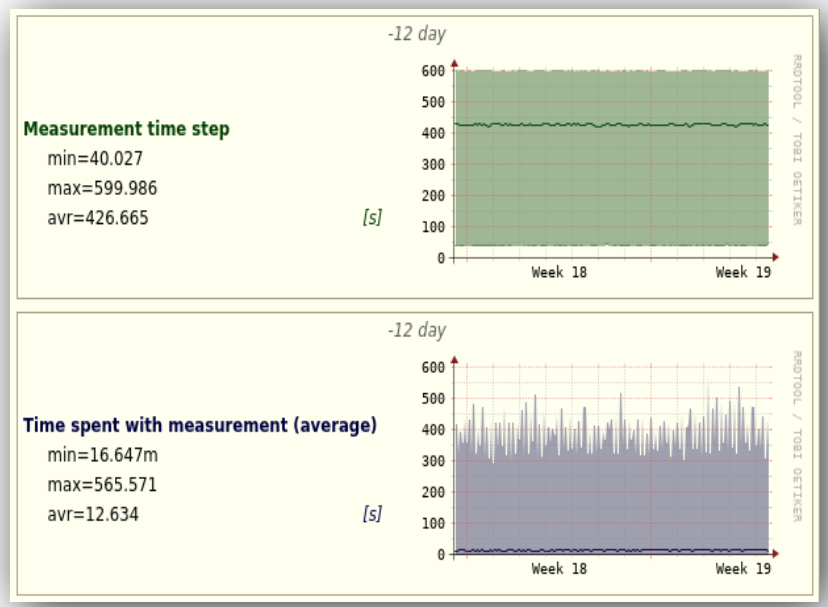
TCP problems

Input errors	min=0.000 max=0.000 avr=0.000	[segments/s]
Segments containing RST flag sent	min=0.000 max=155.339m avr=41.181m	[segments/s]



systém G3

- v e-infrastruktuře CESNET
  - zařízení e-infrastruktury (+ vybraná zařízení uživatelů)
    - aktuálně měřeno
      - ~ 110+ zařízení
      - ~ 8000+ síťových rozhraní
      - ~ 4000 HW komponent



- v sítích uživatelů
  - samostatné instalace
    - na zdrojích uživatelů, v sítích uživatelů

Monitoring provozu

- co nám v té síti běží ?
- využití provozních informací na bázi toků ~ *NetFlow..*
- potřeba přiměřeně detailního obrazu provozu
- potřeba souvislého a plošného sledování provozu
- schopnost zpětně analyzovat datové toky
- + detekce provozních anomálií
- ++ reakce na detekované anomální chování

Monitoring provozu

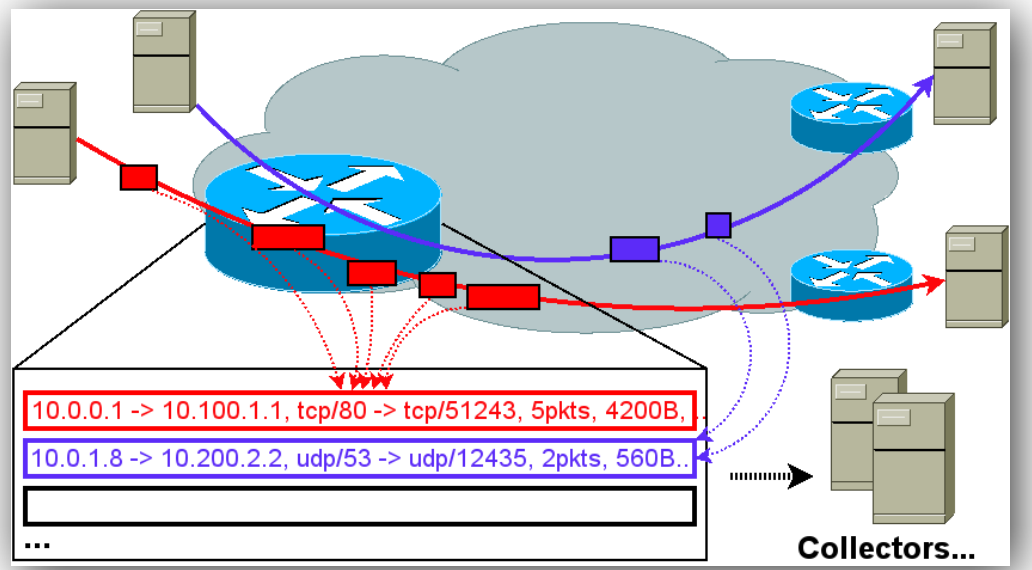
- **provozní informace** ~ *NetFlow, IPFIX, ..sFlow*
  - aktivní síťové prvky
  - sondy HW (např. FlowMon)
  - sondy SW (on the line/on host) ~ **ipfixprobe**, softflowd
    - CESNET/ipfixprobe → https://github.com/CESNET/ipfixprobe
- **zpracování provozních informací**
  - komerční/open source nástroje (Nfsen, flow-tools, FlowMon, .., Akvorado, FastNetMon, ..)
  - řada komerčních nástrojů s FREE TRIAL (někdy volně dostupná verze s omezenými funkcemi)
  - některé nástroje i s detekčními funkcemi

Provozní informace na bázi toků

- informace vybrané z protokolárních hlaviček
  - dočasně agregované v místě vzniku (aktivní síťové prvky, sondy)
  - následně exportované (přirozeně x nuceně) do míst zpracování (tzv. kolektory)

  ~ **NetFlow, IPFIX**
- informace vybrané ze vzorků paketů exportovaných jako součást komplexního monitoringu zařízení

  ~ **sFlow**
- *...v principu a v základu jde vždy o informaci o jednom směru přenosu*



Informační obsah

- typicky závislé na typu zařízení, které informaci vytváří, jeho pozici a funkci
- **síťový prvek**
  - nemusí zvládnout 100% provozu
  - **+ informace o doručení**
    - ano/ne proč ?
    - kudy (vstupní/výstupní rozhraní)
- **sonda**
  - zpravidla zvládne 100% provozu
    - - vidí „medium“ – bez informací o doručení a směrech
    - + detailnější informace ze “sousedních vrstev”
      - exaktní → zpravidla v závislosti na šifrování
      - odvozené → statistika, charakteristika provozu

co+jak+kudy

```
flow_direction=ingress
forwarding_status=forwarded
src_ip=2a02:598:2:0:x:x:x:x
dst_ip=2a07:8d80:f003:101:x:x:x:x
proto=tcp (6)
src_port=https (443)
dst_port=36403
src_if=156
dst_if=49
src_vrfid=0x60000000
dst_vrfid=0x60000000
src_as=43037
dst_as=2852
tos=00000000
tcp_flags=push(8),ack(16)
nexthop=0:0:0:0:0:x:x:x
first=2020/07/25 08:17:29.102
last=2020/07/25 08:17:31.462
octets=34165
pkts=25
```

CO+kudy

```
src_ip=2a02:598:2:0:x:x:x:x
dst_ip=2a07:8d80:f003:101:x:x:x:x
proto=tcp (6)
src_port=https (443)
dst_port=36403
tos=00000000
tcp_flags=push(8),ack(16)
first=2020/07/25 08:17:29.102
last=2020/07/25 08:17:31.462
octets=34165
pkts=25
```

Informační obsah

- příklad netflow dat **ze směrovače (s běžícím BGP)**

Flow-Direction	FWD-Status	Flow-Labelv6	IP-Version	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port
egress	Forwarded		4	147.231.x.x	157.240.x.x	tcp (6)	53483	https (443)
egress	Forwarded		4	142.251.x.x	78.128.x.x	udp (17)	https (443)	60867
egress	Forwarded	67029	6	2a03:2880:x:83:x:x:x:x	2001:718:x:9:x:x:x:x	tcp (6)	https (443)	51881
egress	Forwarded		4	142.251.x.x	193.84.x.x	udp (17)	https (443)	54622
egress	Forwarded	188632	6	2001:718:x:ce:x:x:x:x	2a00:1450:x:80e:x:x:x:x	udp (17)	53952	https (443)

Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Egress-VRFID	Src/Prev-AS	Dst/Next-AS	Src-Bitmask	Dst-Bitmask	TOS-flags	TCP-flags	Nexthop
128	362	0x60000000	0x60000000	AS65001	AS32934	16	24	00000000	ack(16)	91.x.x.x
278	128	0x60000000	0x60000000	AS13074	AS65001	24	19	00000000		195.x.x.x
157	181	0x60000000	0x60000000	AS32934	AS65009	48	48	00000000	push(8), ack(16)	2001:x:x:x:x:x:x:x
278	312	0x60000000	0x60000000	AS13074	AS65004	24	21	00000000		195.x.x.x
171	213	0x60000000	0x60000000		AS15169	48	48	00000000		2001:x:x:x:x:x:x:x
362	171	0x60000000	0x60000000	AS32934	AS65002	24	16	00000000	push(8), ack(16)	195.x.x.x
128	213	0x60000000	0x60000							
213	128	0x60000000	0x60000							
128	362	0x60000000	0x60000							
362	157	0x60000000	0x60000							

Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured	Avr-Pkt-Length
24/05/09 15:57:12.370	24/05/09 15:57:23.354	104.000 B	2.000 p	52
24/05/09 15:57:12.483	24/05/09 15:57:24.452	146.000 B	2.000 p	73
24/05/09 15:57:12.943	24/05/09 15:57:22.026	42.183 KB	36.000 p	1171.75
24/05/09 15:57:13.100	24/05/09 15:57:29.816	641.000 B	8.000 p	80.12
24/05/09 15:57:13.106	24/05/09 15:57:22.736	243.000 B	3.000 p	81

Informační obsah

- příklad netflow dat **z překladového prvku**

Flow-Direction	FW-Event	IP-Version	Src-IP	Dst-IP	Src-PostNAT-IP	Dst-PostNAT-IP	Protocol	Src-Port
ingress	Flow update	4	10.25.x.x	20.33.x.x	195.113.x.x	20.33.x.x	tcp (6)	38470
ingress	Flow update	4	172.30.x.x	158.115.x.x	195.113.x.x	158.115.x.x	udp (17)	44441
ingress	Flow update	4	158.115.x.x	195.113.x.x	158.115.x.x	172.30.x.x	udp (17)	7351
ingress	Flow update	4	172.25.x.x	195.113.x.x	195.113.x.x	195.113.x.x	udp (17)	44778
ingress	Flow update	4	172.30.x.x	158.115.x.x	195.113.x.x	158.115.x.x	udp (17)	44356
ingress	Flow update	4	158.115.x.x	195.113.x.x	158.115.x.x	172.30.x.x	udp (17)	7351
ingress	Flow update	4	172.25.x.x	34.160.x.x	195.113.x.x	34.160.x.x	tcp (6)	32855
ingress	Flow update	4	34.160.x.x	195.113.x.x	34.160.x.x	172.25.x.x	tcp (6)	https (443)

Dst-Port	Src-PostNAPTPort	Dst-PostNAPTPort	Src-ifIndex	Dst-ifIndex	TOS-flags	TCP-flags	Bytes-measured	Pkts-measured
xmpp-client (5222)	24659	xmpp-client (5222)	101010911	10	00000000	syn(2), push(8), ack(16)	82.000 B	1.000 p
7351	42828	7351	101020912	10	00000000		474.000 B	3.000 p
42828	7351	44441	10	101020912	00000000		264.000 B	3.000 p
65101	44778	65101	9	10	00000000		423.047 KB	320.000 p
7351	59417	7351	101010911	10	00000000		474.000 B	3.000 p
59417	7351	44356	10	101010911	00000000		264.000 B	3.000 p
https (443)	32855	https (443)	9	10	00000000	push(8), ack(16)	264.000 B	4.000 p
32855	https (443)	32855	10	9	00000000	push(8), ack(16)	264.000 B	4.000 p
47594	https (443)	47594	10	9	00000000	syn(2), push(8), ack(16)	264.000 B	4.000 p

Informační obsah

- příklad dat **z ipfixprobe (obsah významně redukovaný monitorovacím systémem)**

Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	VLAN-ID	Src-MAC-Addr	Dst-MAC-Addr	TCP-flags
157.240.x.x	195.113.x.x	udp (17)	https (443)	35869	21	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b2	
195.93.x.x	52.97.x.x	tcp (6)	https (443)	50525		38:22:d6:b8:95:b1	d4:eb:68:d4:7b:53	syn(2), push(8), ack(16), ece(64)
157.240.x.x	195.113.x.x	udp (17)	https (443)	53629	21	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b2	
157.240.x.x	195.113.x.x	udp (17)	https (443)	33673	21	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b2	
84.17.x.x	195.113.x.x	tcp (6)	https (443)	61389	21	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b2	syn(2), push(8), ack(16)
185.41.x.x	195.113.x.x	tcp (6)	https (443)	62861	21	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b2	syn(2), push(8), ack(16)
157.240.x.x	195.93.x.x	tcp (6)	https (443)	59732	20	d4:eb:68:d4:7b:53	38:22:d6:b8:95:b1	syn(2), push(8), ack(16)
157.240								
157.240								
157.240								

SNI	Min-TTL	Max-TTL	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured
	58	58	24/05/13 09:35:43.158	24/05/13 09:40:40.936	190.295 MB	152.722 Kp
vsocina.cz	122	122	24/05/13 09:35:47.726	24/05/13 09:40:46.974	189.497 MB	134.217 Kp
	58	58	24/05/13 09:36:16.196	24/05/13 09:41:15.535	188.060 MB	150.474 Kp
	58	58	24/05/13 09:35:50.224	24/05/13 09:40:49.952	164.186 MB	131.464 Kp
	59	59	24/05/13 09:36:14.707	24/05/13 09:40:36.931	154.445 MB	109.045 Kp
)-prod06-live.solocoo.tv	61	61	24/05/13 09:35:42.217	24/05/13 09:40:40.830	135.473 MB	91.897 Kp
	58	58	24/05/13 09:35:47.440	24/05/13 09:40:46.354	116.779 MB	83.239 Kp
prg1-1.xx.fbcdn.net	58	58	24/05/13 09:36:07.133	24/05/13 09:41:06.033	101.264 MB	77.825 Kp
prg1-1.cdninstagram.com	58	58	24/05/13 09:35:34.319	24/05/13 09:40:30.541	75.026 MB	53.454 Kp
prg1-1.cdninstagram.com	58	58	24/05/13 09:36:24.904	24/05/13 09:41:18.053	71.854 MB	51.306 Kp

Informační obsah

- příklad **sflow** dat

Flow-Direction	FWD-Status	IP-Version	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	VLAN-ID
ingress	Forwarded	4	160.x.x.x	160.x.x.x	tcp (6)	microsoft-ds (445)	49928	127	0	210
ingress	Forwarded	4	160.x.x.x	160.x.x.x	tcp (6)	microsoft-ds (445)	49800	127	0	210
ingress	Forwarded	4	160.x.x.x	160.x.x.x	gre (47)			140	0	82
ingress	Forwarded	4	160.x.x.x	160.x.x.x	tcp (6)	1526	36218	118	0	285
ingress	Forwarded	4	160.x.x.x	160.x.x.x	gre (47)			140	0	82
ingress	Forwarded	4	160.x.x.x	160.x.x.x	tcp (6)	microsoft-ds (445)	56228	118	0	6
ingress	Forwarded	4	160.x.x.x	160.x.x.x	gre (47)			140	0	82
ingress	Forwarded	4	160.x.x.x	160.x.x.x	gre (47)			140	0	82
ingress	Forwar									

Src-MAC-Addr	Dst-MAC-Addr	TOS-flags	TCP-flags	Min-TTL	Max-TTL	Bytes-measured	Pkts-measured
f8:bc:12:12:6e:e0	d0:7e:28:43:65:00	00000000	push(8), ack(16)	128	128	33.772 KB	23.000 p
f8:bc:12:12:6e:e0	d0:7e:28:43:65:00	00000000	push(8), ack(16)	128	128	19.028 KB	17.000 p
00:1a:1e:04:94:50	d0:7e:28:43:65:00	00000000		255	255	18.000 KB	12.000 p
00:25:90:b9:15:ff	d0:7e:28:43:65:00	00000000	push(8), ack(16)	63	63	15.441 KB	11.000 p
00:1a:1e:04:94:50	d0:7e:28:43:65:00	00000000		254	254	15.216 KB	14.000 p
00:15:5d:07:67:db	d0:7e:28:43:65:00	00000000	ack(16)	128	128	15.000 KB	10.000 p
00:1a:1e:04:94:50	d0:7e:28:43:65:00	00000000		255	255	15.000 KB	10.000 p
00:1a:1e:04:94:50	9c:8c:d8:c2:0c:56	00000000		255	255	14.872 KB	11.000 p
cc:90:70:7f:63:3c	d0:7e:28:43:65:1f	00000000		61	61	14.058 KB	11.000 p

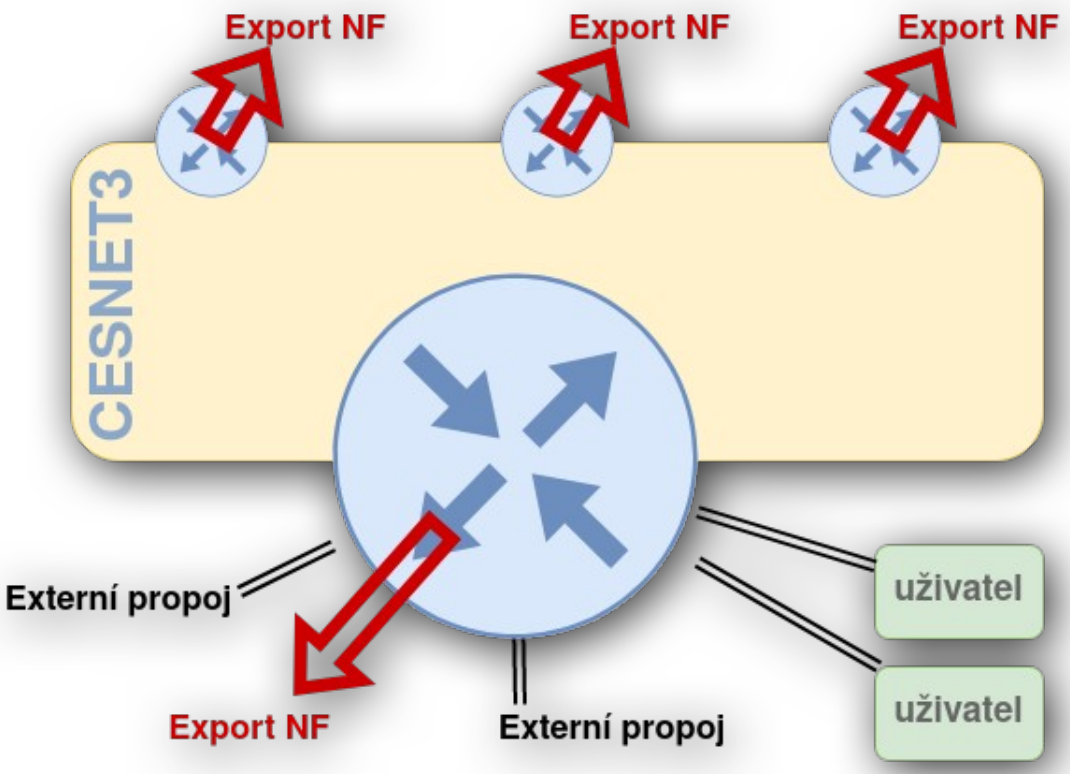
Důležité parametry

- **timeout ~ TTL pro uchování záznamu ve flow-cache**
  - active, inactive; v případě zaplnění paměti → nucený export
- **vzorkování – sampling**
  - 1:X, paketová perspektiva - řízená ztráta vypovídací hodnoty → spotřeba zdrojů v přijatelném pásmu (především aktivní síťové prvky)
  - když zařízení nestíhá v rámci nastavených parametrů, začne neřízeně zahazovat (flow-engine – propustnost, flow-cache – velikost)
  - sondy většinou konstruované na „wire-speed" → "selling-point"
- **obecně pro naplnění účelu, který od toho chceme**
  - nerozhoduje pouze výkon zdroje, ale celý řetězec zpracování
    - absorpční schopnost
    - schopnost pracovat se vzorkovanými daty

V e-infrastruktuře CESNET

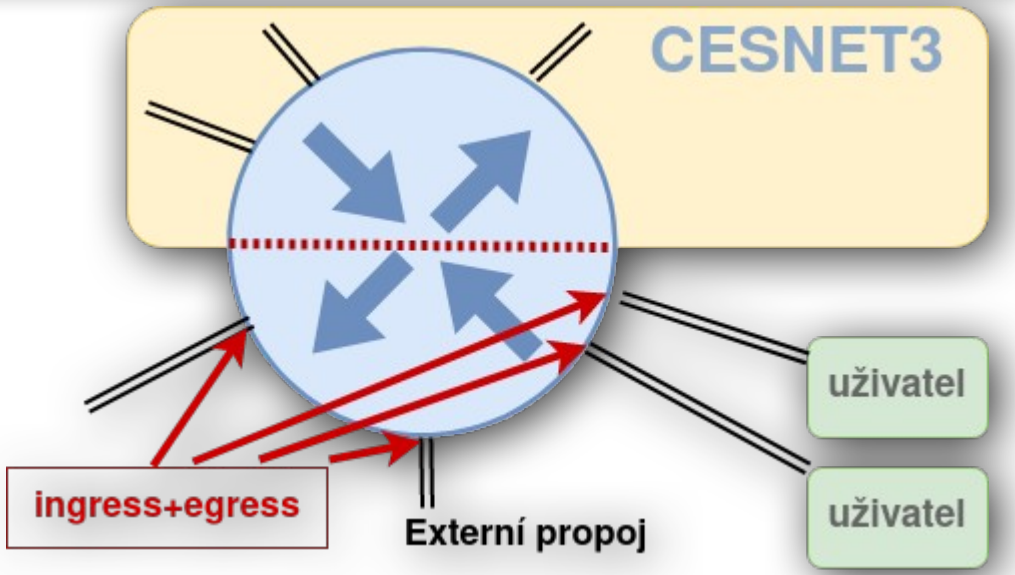
- permanentní zdroje
  - páteřní směrovače (MPLS-PE, MPLS-CE)
    - ~ všechny hraniční – „obvod páteře“
  - NetFlow v9, v10/IPFIX

- on-demand
  - sondy na externích linkách
  - potenciální záloha, pro případný selektivní detailní sběr informací
  - NetFlow v9, IPFIX



V e-infrastruktuře CESNET

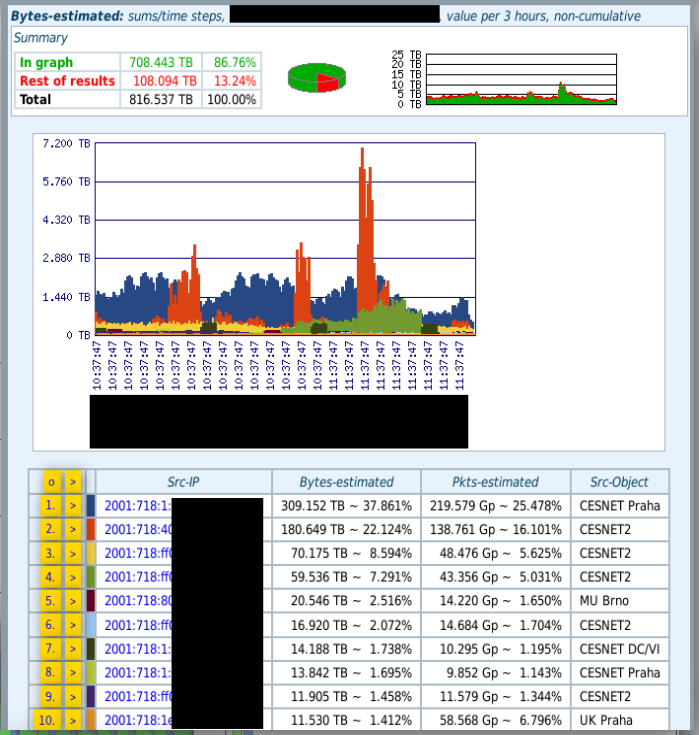
- nastavení zpracování NetFlow na páteřních směrovačích
  - ne rozhraní do jádra
  - všechna klientská a externí rozhraní
  - zpracování egress+ingress provozu
  - ingress - netflow z provozu, který vstupuje rozhraním do zařízení
  - egress - netflow z provozu, který vystupuje rozhraním ze zařízení

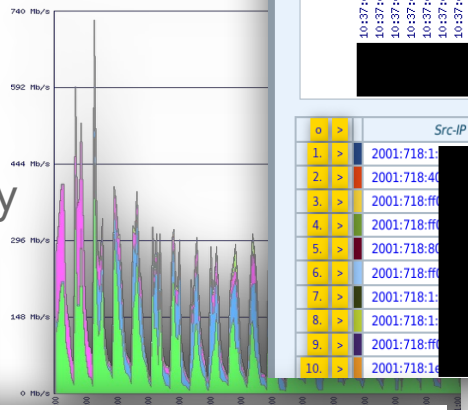


Monitoring provozu

Systém FTAS

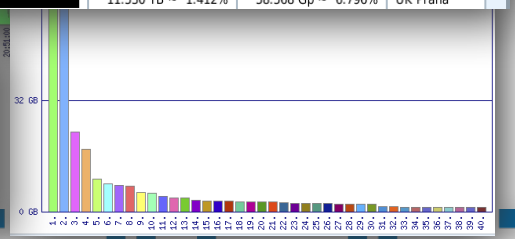
- vyvíjen pro vlastní potřeby monitoringu páteřní sítě
- sběr, zpracování, uchování, vizualizace provozních informací
  - dlouhodobé uchování dat (vč. podpory plnění legislativních požadavků)
  - klasifikace, třídění, agregační funkce
  - detekční funkce, regulace provozu
  - analýzy provozu, statistické vyhodnocení, trendy



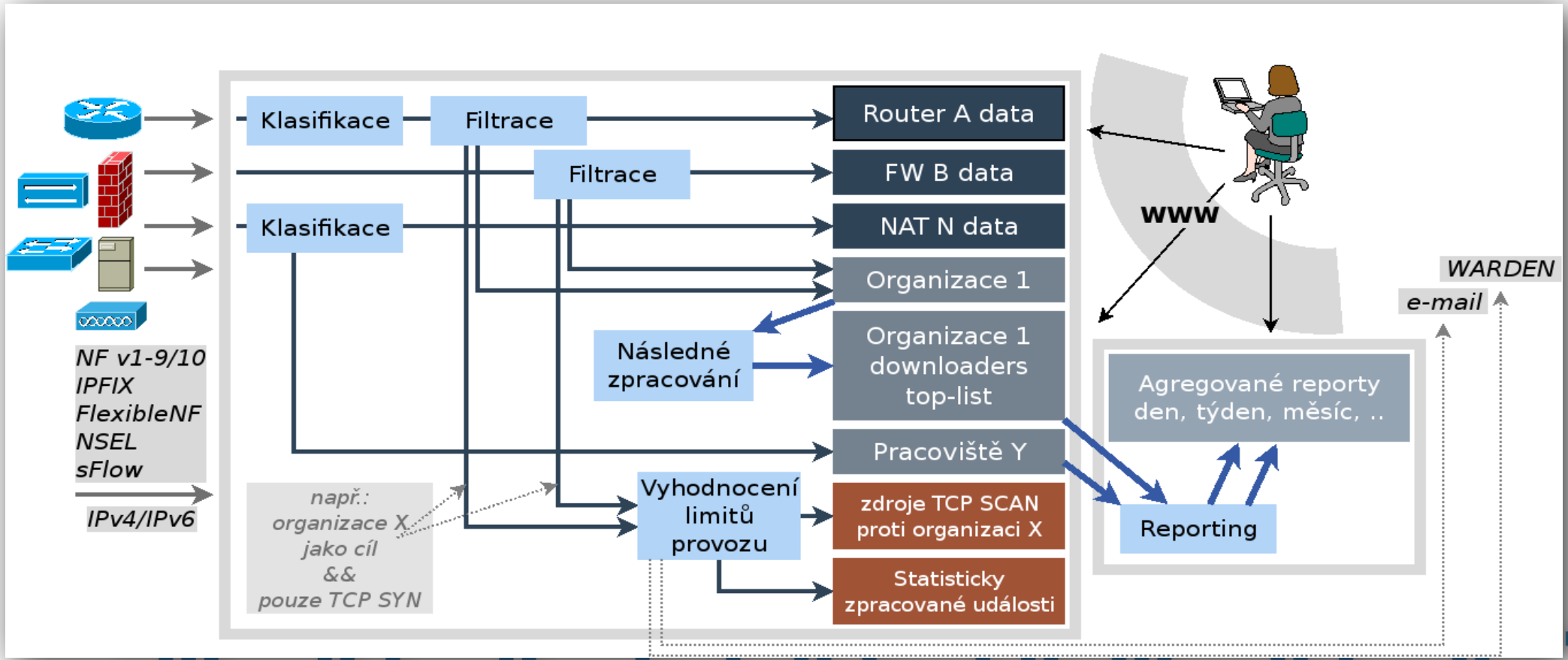


o	Flow-Direction	FWD-Status	Src-IP	Protocol	Src-Port	Src-ifIndex	Dst-ifIndex	Src/Prev-AS	TOS-flags	Bytes-estimated	Pkts-estimated	Flow-Cnt
1.	ingress	Forwarded	77.75.[redacted]	tcp (6)	https (443)	156	49	AS43037	10101010	3.073 GB	2.844 Mp	26319
2.	ingress	Forwarded	77.75.[redacted]	tcp (6)	https (443)	156	140	AS43037	00000010	693.980 MB	636.120 Kp	6119
3.	ingress	Forwarded	2a02:5[redacted]:0:79:53	tcp (6)	https (443)	156	49		00000010	476.113 MB	444.960 Kp	4659
4.	ingress	Forwarded	2a02:5[redacted]:0:79:53	tcp (6)	https (443)	156	140		00000010	95.478 MB	88.600 Kp	929
5.	ingress	Forwarded	77.75.[redacted]	tcp (6)	https (443)	156	105	AS43037	00000010	73.180 MB	67.560 Kp	683
6.	ingress	Forwarded	108.17[redacted]	tcp (6)	https (443)	94742	49	AS15169	00000000	57.358 MB	72.400 Kp	492
7.	ingress	Forwarded	108.17[redacted]	tcp (6)	https (443)	94742	49	AS15169	00000000	34.228 MB	49.440 Kp	454

```
# Src-IP;Src-GeoIP;Bytes-estimated;Bytes-estimated-Percent;Pkts-estimated;Pkts-estimated-Percent;Flow-Cnt;Flow-Cnt-Percent;Detector-Type;Detector-Name
# src_ip;src_ip_cc;statist_octets;statist_octets_percent;statist_pkts;statist_pkts_percent;flowcnt;flowcnt_percent;detector_type;detector
185.22[redacted]1;;666308800;0.0800714469973045;16657720;0.0802009849319872;416443;0.0801883512289643;Src-IP;TCP SYN against internal IP address ranges, sources
80.82.[redacted]YC;589342400;0.0708222655094218;14733560;0.0709368403091497;368339;0.0709256659454607;Src-IP;TCP SYN against internal IP address ranges, sources
5.188.[redacted]RUS;539766400;0.0648646343685178;13494160;0.0649695710355213;337354;0.0649593366691144;Src-IP;TCP SYN against internal IP address ranges, sources
5.8.18[redacted];431857600;0.0518970527310807;10796440;0.0519810107120965;269911;0.0519728223755976;Src-IP;TCP SYN against internal IP address ranges, sources
80.82.[redacted]YC;412067200;0.0495188071418653;10301680;0.0495989176462417;257542;0.0495911045502264;Src-IP;TCP SYN against internal IP address ranges, sources
5.8.18[redacted];399057600;0.0479554216712604;9976440;0.0480330029628829;249411;0.0480254365384151;Src-IP;TCP SYN against internal IP address ranges, sources
5.188.[redacted]RUS;390915200;0.0469769357949958;9772880;0.0470529341123587;244322;0.0470455220737604;Src-IP;TCP SYN against internal IP address ranges, sources
```

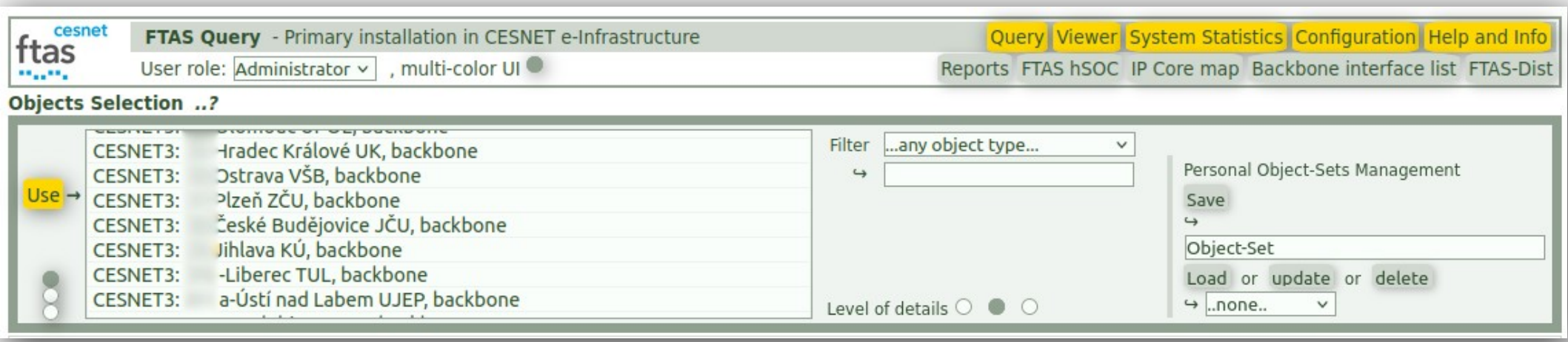


Systém FTAS – zpracování, uchování a zpřístupnění provozních informací na bázi toků



Systém FTAS

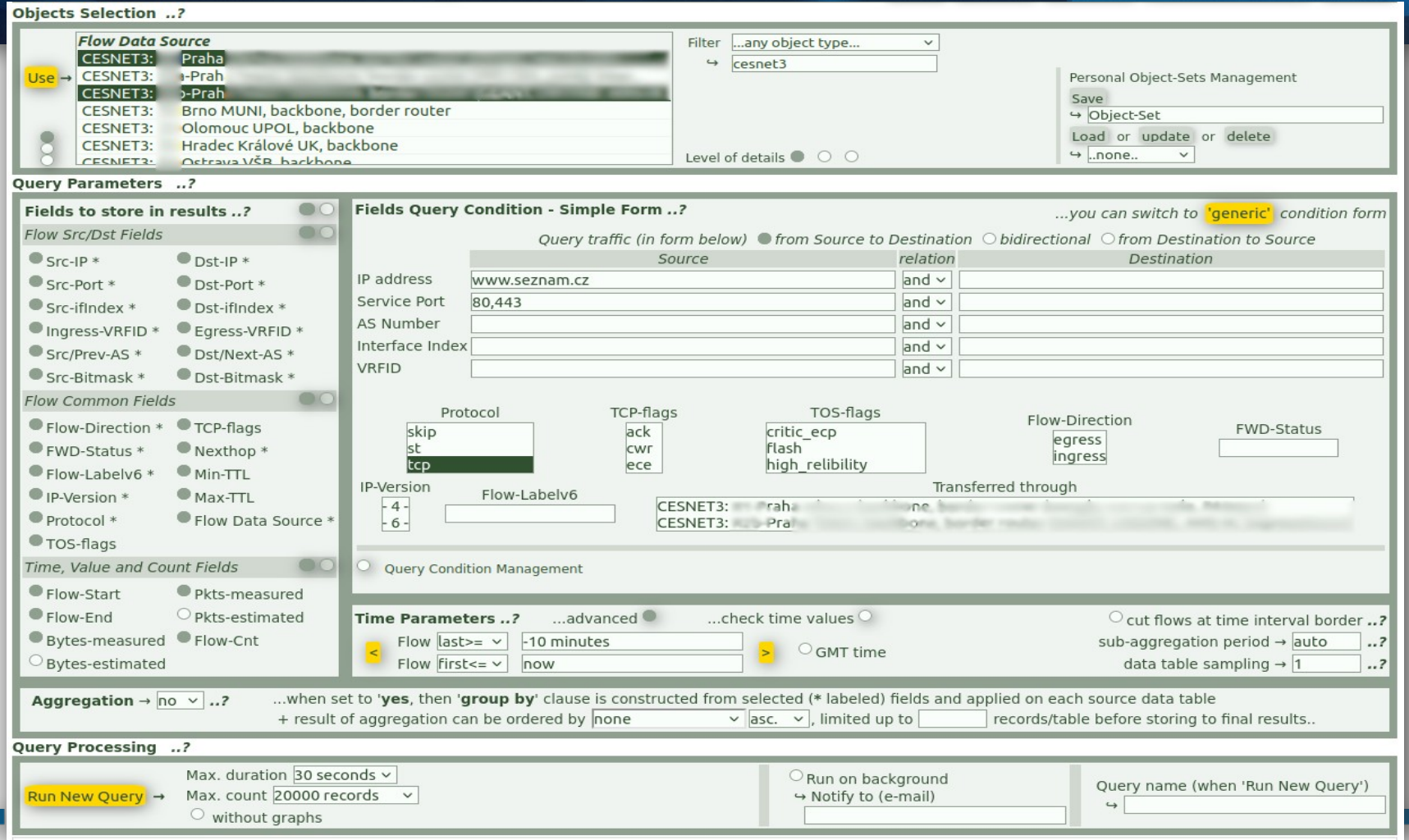
- ukázky UI
- výber zdrojů dat



Monitoring provozu

Systém FTAS

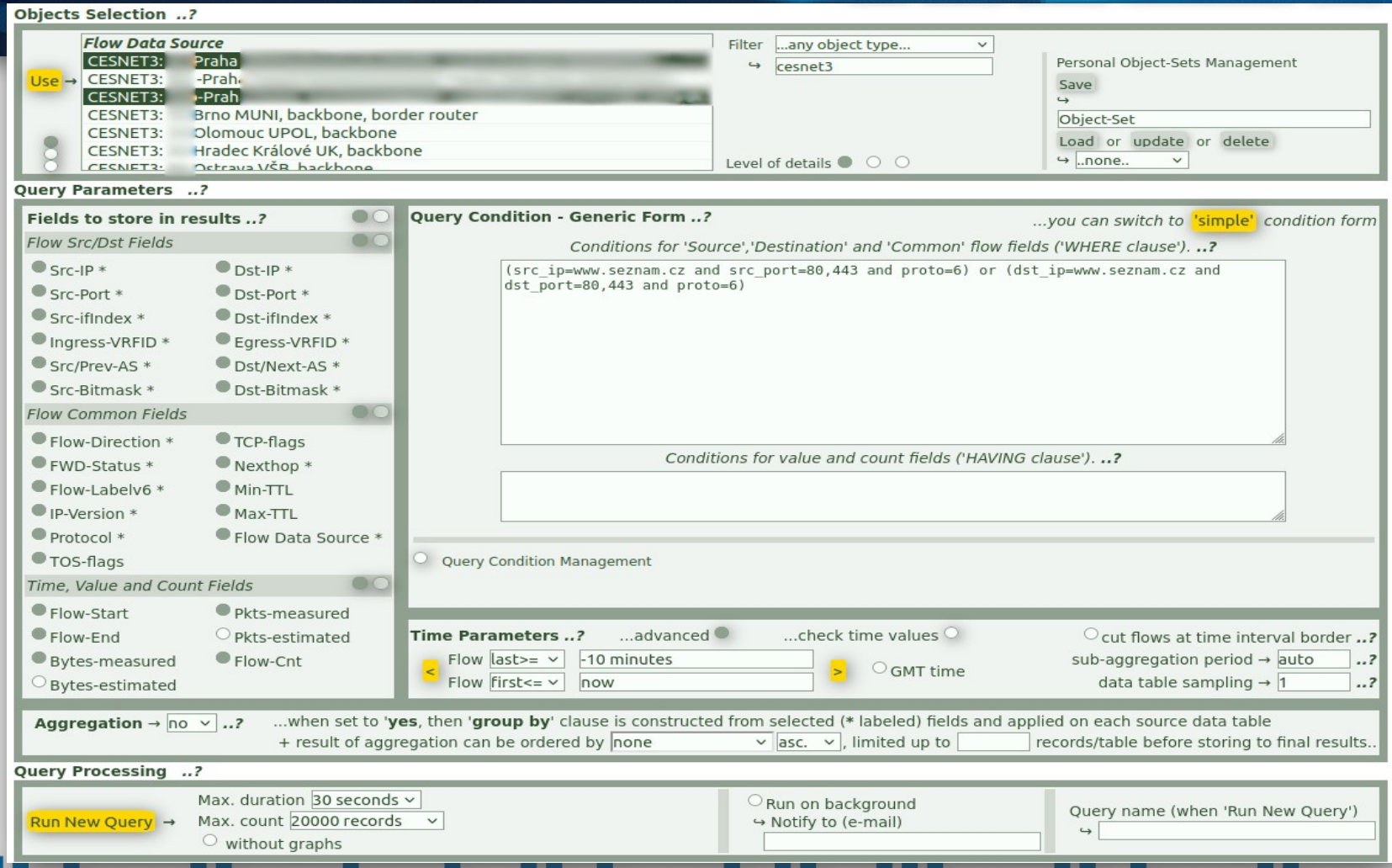
- ukázky UI
- vyhledávání



Monitoring provozu

Systém FTAS

- ukázky UI
- vyhledávání



Systém FTAS

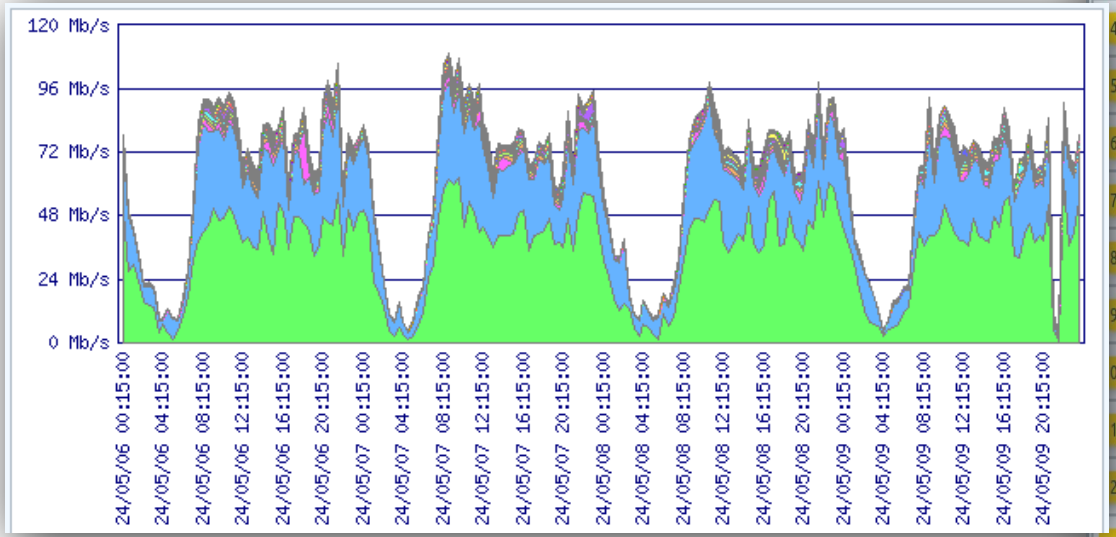
- ukázky UI - vizualizace

Flow-Direction	FWD-Status	IP-Version	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRFID	Egress-VRFID
egress	Forwarded	4	77.75.79.222 www.seznam.cz	193.84.36.x ---.czu.cz	tcp (6)	https (443)	38682	362	312	0x60000000	0x60000000
egress	Forwarded	4	77.75.79.222 www.seznam.cz	193.84.36.x ---.czu.cz	tcp (6)	https (443)	65087	362	312	0x60000000	0x60000000
egress	Forwarded	4	77.75.79.222 www.seznam.cz	193.84.36.x ---.czu.cz	tcp (6)	https (443)	50010	362	312	0x60000000	0x60000000
egress	Forwarded	4	77.75.79.222 www.seznam.cz	193.84.36.x	tcp (6)	https (443)	63905	362	312	0x60000000	0x60000000
egress	Forwarded	4	77.75.79.222 www.seznam.cz	193.84.36.x ---.czu.cz	tcp (6)	https (443)	64957	362	312	0x60000000	0x60000000

AS43037	AS65004	23	21	00000000	push(8), ack(16)	24/05/13 10:34:11.047	4.308 MB	3.783 Kp
AS43037	AS65004	23	21	00000000	push(8), ack(16)	24/05/13 10:31:07.387	4.119 MB	4.483 Kp
AS43037	AS65004	23	21	00000000	push(8), ack(16)	24/05/13 10:34:16.525	3.298 MB	2.998 Kp
AS43037	AS65004	23	21	00000000	push(8), ack(16)	24/05/13 10:32:01.254	2.484 MB	2.179 Kp
AS43037	AS65004	23	21	00000000	push(8), ack(16)	24/05/13 10:35:00.731	1.844 MB	1.940 Kp

Systém FTAS

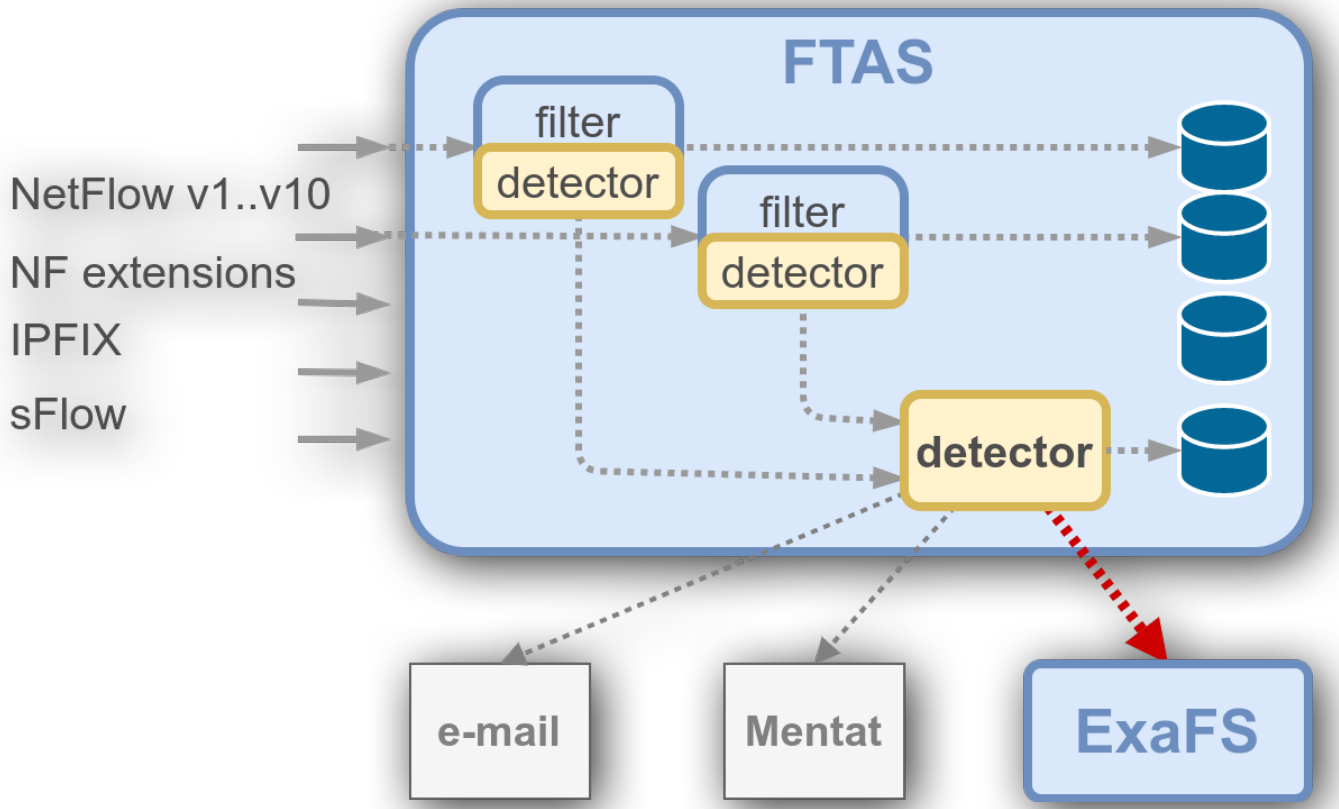
- ukázky UI - vizualizace



o	Flow-Direction	FWD-Status	IP-Version	Src-IP	Protocol	Src-Port	Bytes-estimated	Dst-IP-Cnt
1.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	1.498 TB	83
2.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	888.931 GB	119
3.	egress	Forwarded	4	[redacted]	tcp (6)	https (443)	64.660 GB	123
4.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	39.866 GB	27
5.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	30.382 GB	97
6.	egress	Forwarded	4	[redacted]	tcp (6)	https (443)	29.187 GB	95
7.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	27.221 GB	36
8.	egress	Forwarded	4	[redacted]	tcp (6)	https (443)	23.407 GB	115
9.	egress	Forwarded	4	[redacted]	udp (17)	3478	16.469 GB	15
0.	egress	Forwarded	4	[redacted]	tcp (6)	https (443)	15.026 GB	34
1.	egress	Forwarded	4	[redacted]	tcp (6)	https (443)	12.838 GB	91
2.	egress	Forwarded	4	[redacted]	udp (17)	https (443)	11.756 GB	78
13.	egress	Forwarded	4	[redacted]	udp (17)	3478	8.565 GB	12
14.	egress	Forwarded	4	[redacted]	udp (17)	3478	6.127 GB	13
15.	egress	Forwarded	4	edge-star-mini-shv-01-prg1.facebook.com	udp (17)	https (443)	6.118 GB	116

Systém FTAS – detekční prvky

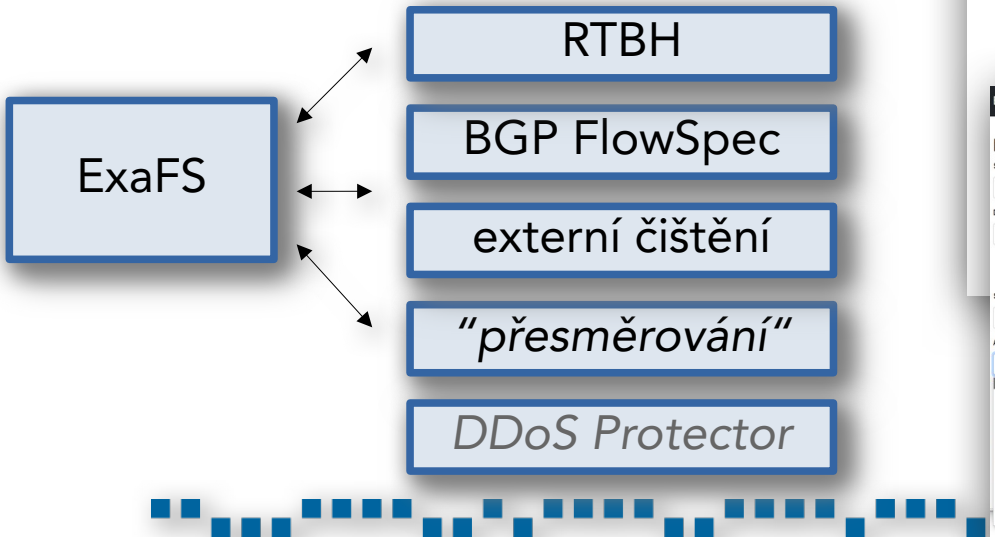
- funkce pro konfiguraci detektorů
- přímé řízení ExaFS (nástroj pro regulaci provozu)
- notifikace

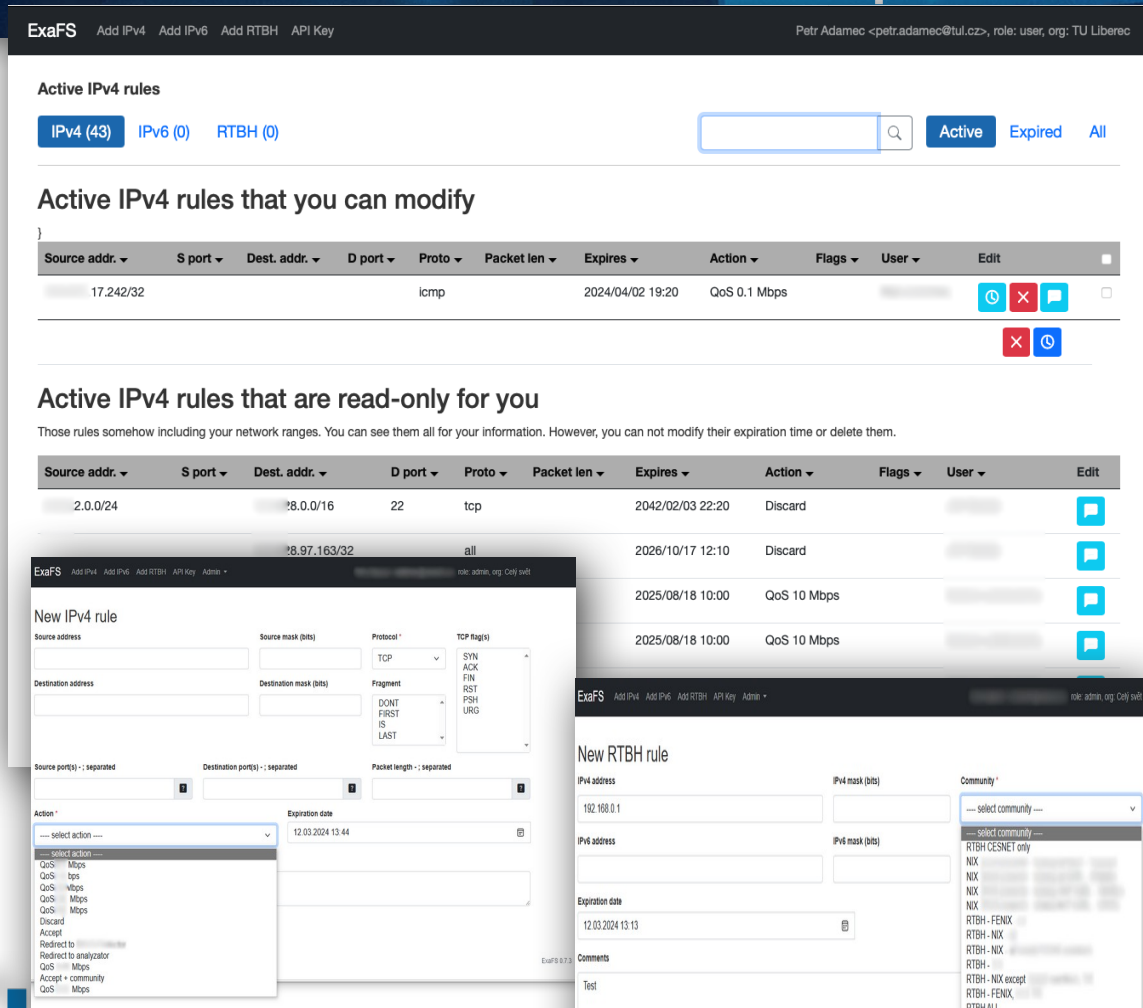


Monitoring provozu a obrana na úrovni transportu

ExaFS

- UI, API
- "central point of knowledge"
- síťové technologie navázané na back-end
- práva strukturována podle prefixů
- tzn. i jako služba pro uživatele

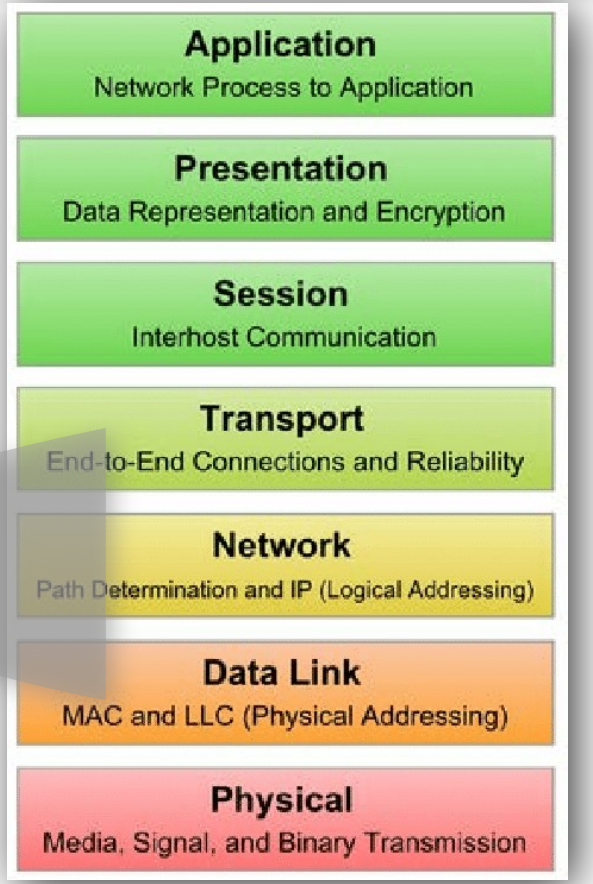




Monitoring provozu a obrana na úrovni transportu

FTAS → obranné role

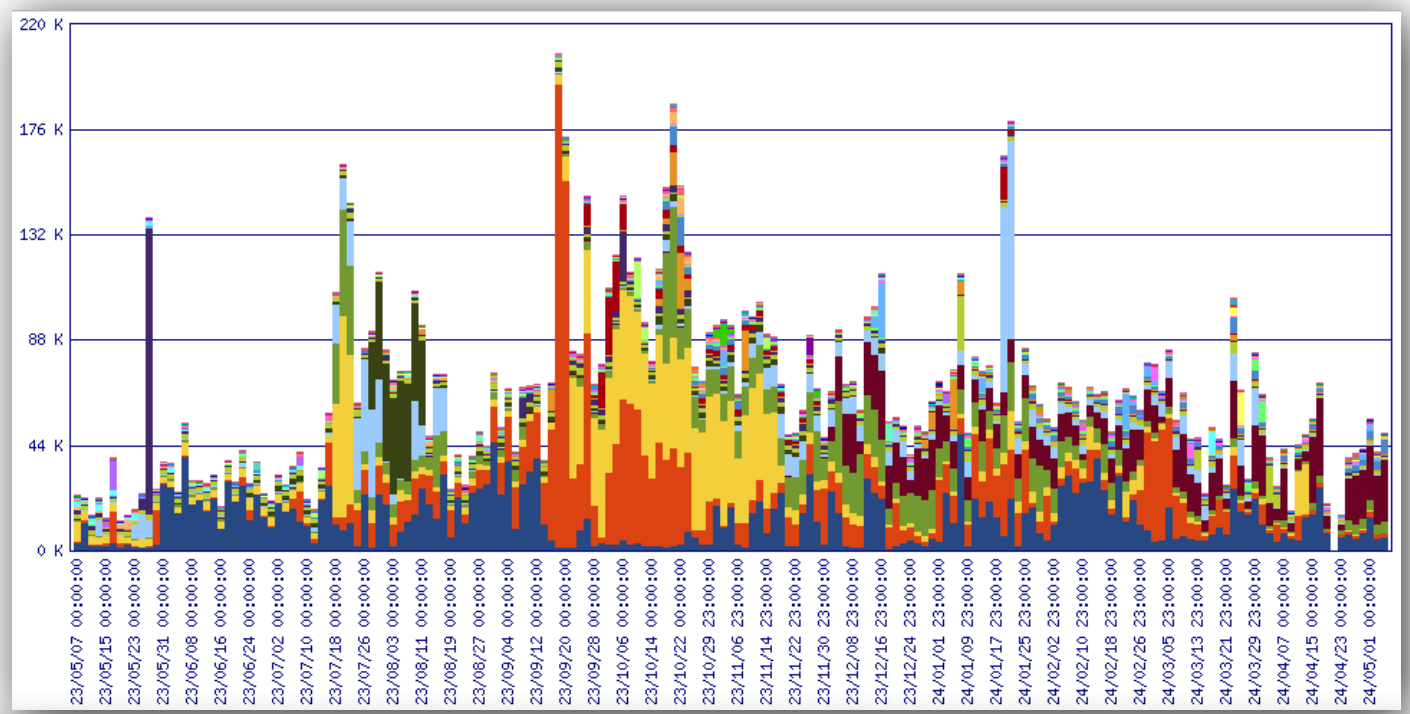
- **automatická obrana proti běžným anomáliím / útokům**
  - „standardní“ vlastnost (součást) služby připojení uživatelů
  - možnost specifických limitů pro konkrétní prefixy
  - možnost “whitelistingu“ ..oznamujte, prosím, případné testování vašich sítí
- **on-demand specifické detektory v případě potřeby**
  - určitá podpora i u aplikačně orientovaných útoků → ale limity monitorovací metody nelze překročit



Monitoring provozu a obrana na úrovni transportu

Systém FTAS

- ukázky UI – vizualizace
- celá komunita
- roční průběh agregátů **detekovaných událostí** za 2 dny – ve špičkách více než 2/s

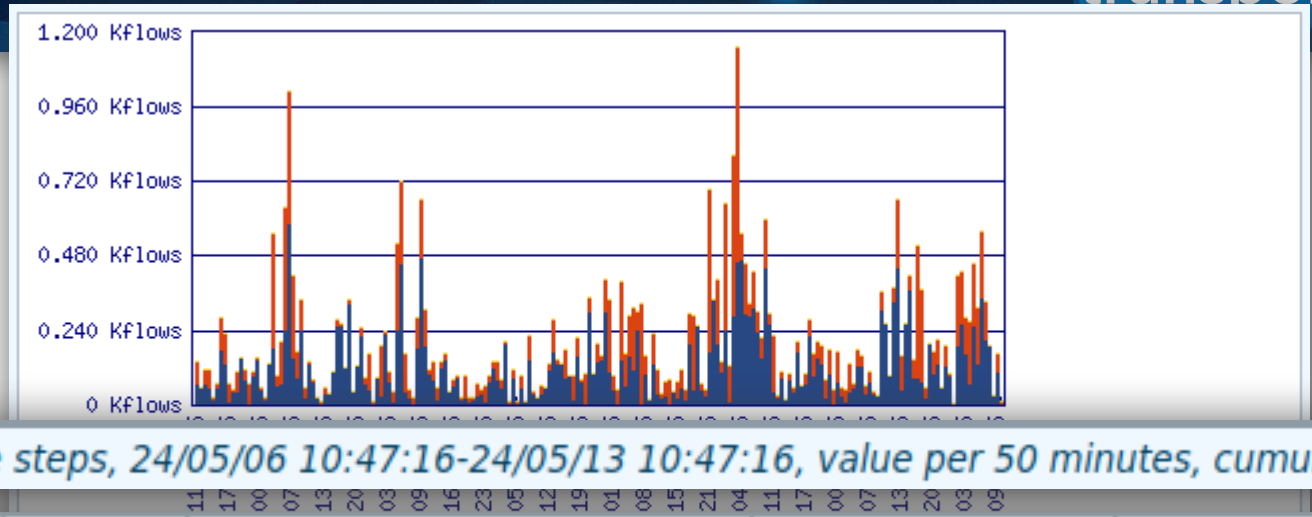


o	Flow-Start [CEST]	Flow-End [CEST]	Bytes-estimated	Src-IP-Cnt	Flow-Cnt	Flow-Cnt-Drop	Detected-Event-Cnt	Detector-Type
1.	23/05/05 23:19:30.000	24/05/06 00:22:58.000	120.099 GB	67129	1962329448	1807462296	12182741	Src-IP

Monitoring provozu a obrana na úrovni transportu

Systém FTAS

- ukázky UI – vizualizace
- specifický detektor (ČZU)



Flow-Cnt: *sums/time steps, 24/05/06 10:47:16-24/05/13 10:47:16, value per 50 minutes, cumulative*

Flow-Direction	FWD-Status	Protocol	TOS-flags	TCP-flags	Flow-Start	Flow-End
ingress	Forwarded	tcp (6)	11111111	fin(1), syn(2), rst(4), push(8), ack(16)	24/05/06 10:47:16.207	24/05/13 10:36:11.968
ingress	Dropped	tcp (6)	11111110	syn(2)	24/05/06 10:50:57.396	24/05/13 10:30:38.968
ingress	Drop ACL Deny	tcp (6)	00000000	syn(2)	24/05/07 05:42:24.966	24/05/07 05:42:25.029

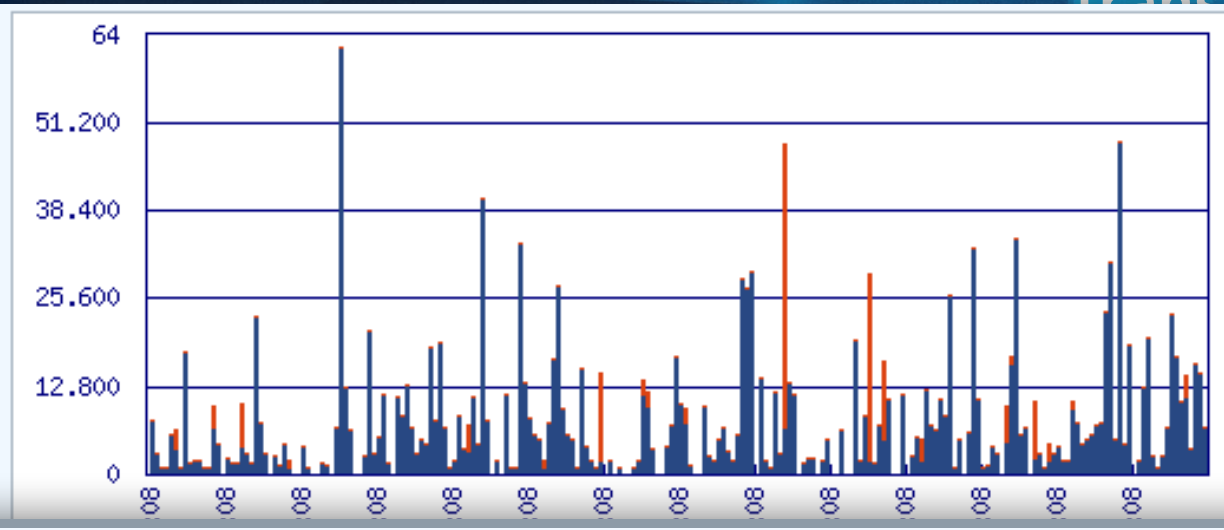
Bytes-estimated	Pkts-estimated	Src-IP-Cnt	Src-Port-Cnt	Avr-Pkt-Length	Flow-Cnt
63.671 MB	1.166 Mp	1807	15865	54.43	24408
29.867 MB	573.404 Kp	173	10949	51.91	15075
10.764 KB	206.000 p	1	2	52	2

cesnet

Monitoring provozu a obrana na úrovni transportu

Systém FTAS

- ukázky UI – vizualizace
- detektory (ČZU)



Detected-Event-Cnt: *sums/time steps, 24/04/15 11:24:08-24/05/13 11:24:08, value per 3 hours, cumulative*

Flow-Start	*Flow-End*	*Bytes-estimated*	*Pkts-estimated*	*Src-IP-Cnt*
24/04/15 11:29:33.000	24/05/13 11:16:30.000	168.027 MB	3.223 Mp	344
24/04/16 03:15:24.000	24/05/12 21:14:33.000	59.514 MB	658.230 Kp	32

Flow-Cnt	*Flow-Cnt-Drop*	*Detected-Event-Cnt*	*Detector-Type*	*Detector-Name*
80718	27679	1550	Src-IP	against CZU
13187	5603	140	Src-IP	against CZU

Provozní informace, FTAS jako služba

- instalace v e-infrastruktuře
  - správa e-infrastruktury
  - služba pro uživatele
    - filtr provozu z páteře → samostatné uchování uživatelských dat + zpřístupnění (ČZU)
    - export provozních informací ze svých zdrojů
- vlastní instalace na prostředcích uživatele
  - společná správa ...→ vlastní správa
  - uživatelé e-infrastruktury, ISP, IXP, veřejná správa, zdravotnictví (komunitní i individuální instalace)

Sondy

- export “obohacených” NetFlow dat
- HW akcelerované
- SW **ipfixprobe** - https://github.com/CESNET/ipfixprobe


cesnet
Díky za pozornost.