



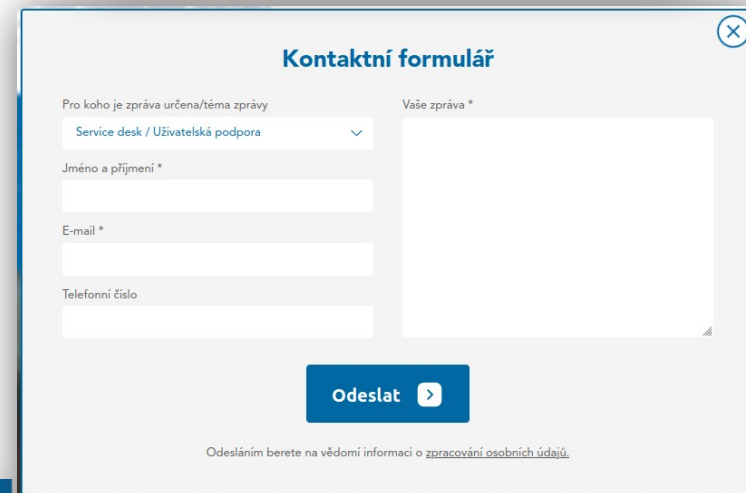
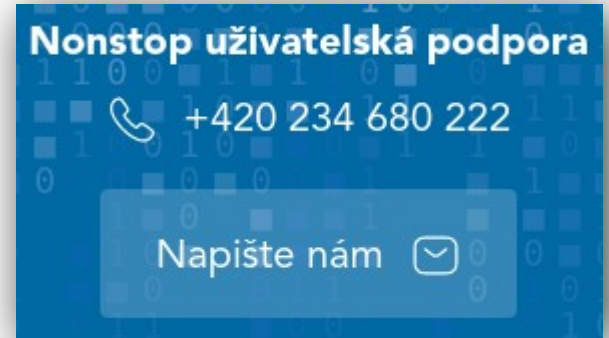
Monitoring a měření

Tomáš Košnar
CESNET

CESNET DAY - ČZU
15. 5. 2024

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

A screenshot of a contact form titled "Kontaktní formulář" in blue. The form has a light gray background and a close button (X) in the top right corner. It contains several input fields: a dropdown menu for "Pro koho je zpráva určena/téma zprávy" (currently showing "Service desk / Uživatelská podpora"), a text field for "Jméno a příjmení *", a text field for "E-mail *", and a text field for "Telefonní číslo". To the right of these fields is a large text area for "Vaše zpráva *". At the bottom center is a blue button with the text "Odeslat" and a white right-pointing arrow. At the very bottom, there is a small line of text: "Odesláním berete na vědomí informaci o [zpracování osobních údajů](#)."

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 ?

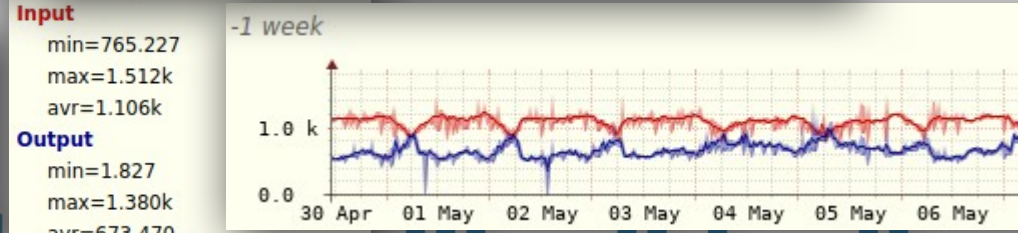
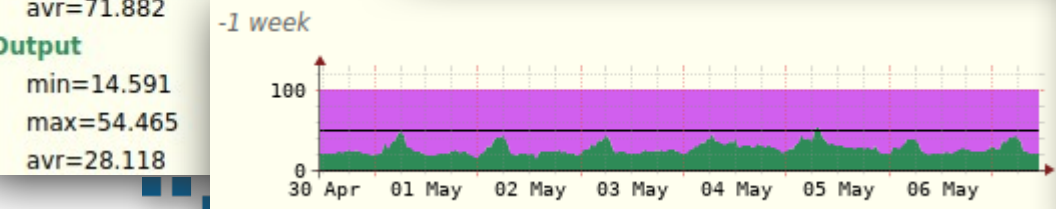
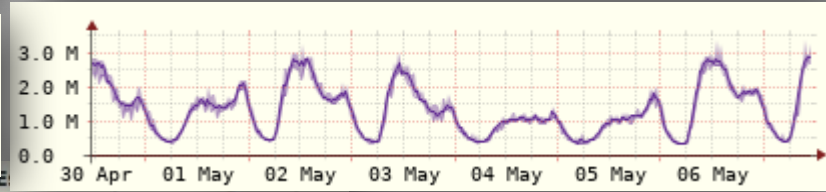
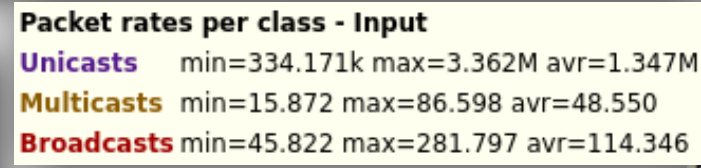
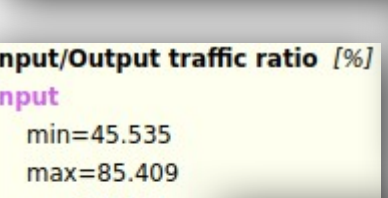
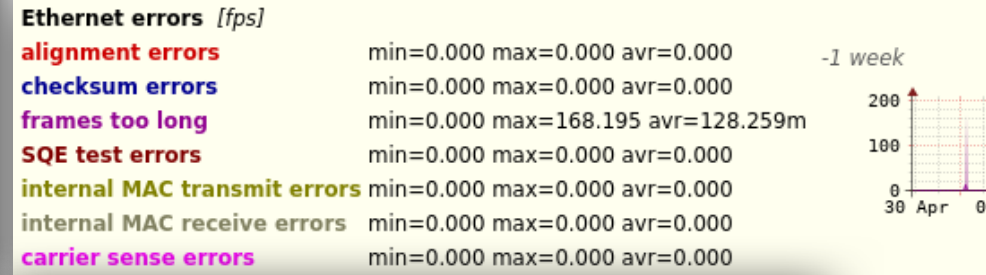
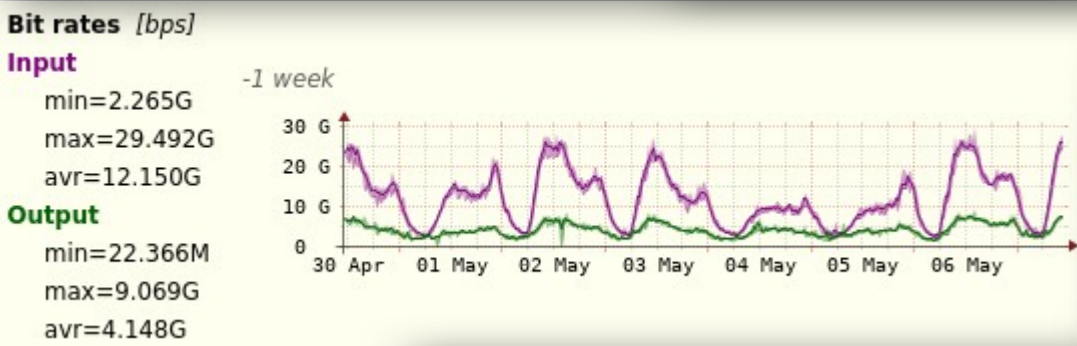
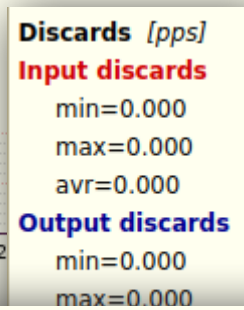
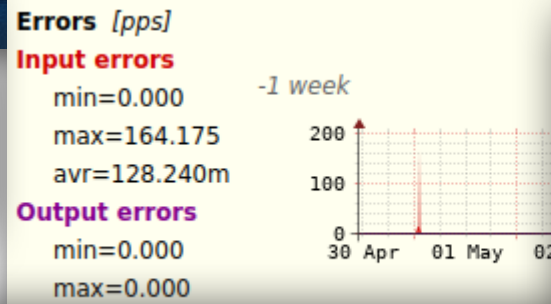
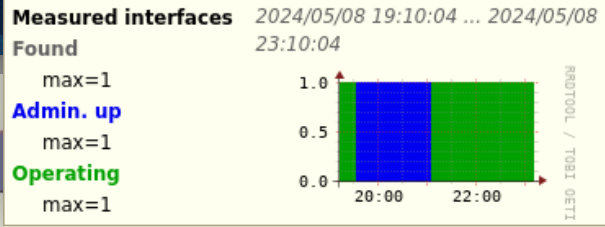
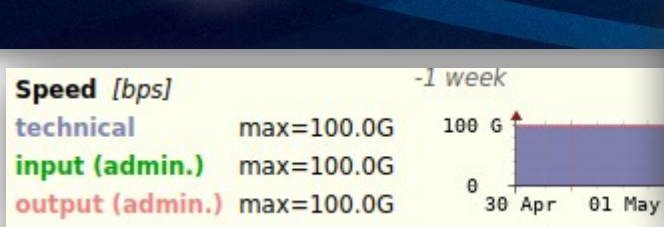
Členění problematiky

- monitoring infrastruktury
 - monitoring provozu
- 
- A decorative horizontal bar at the bottom of the slide consisting of a series of small, blue, square-shaped elements of varying heights and positions, creating a pixelated or digital effect.

Smysl, potřeba

- 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 zhlásit překročení nastavených limitů (zátěž, chybovost,..), změny stavů ..



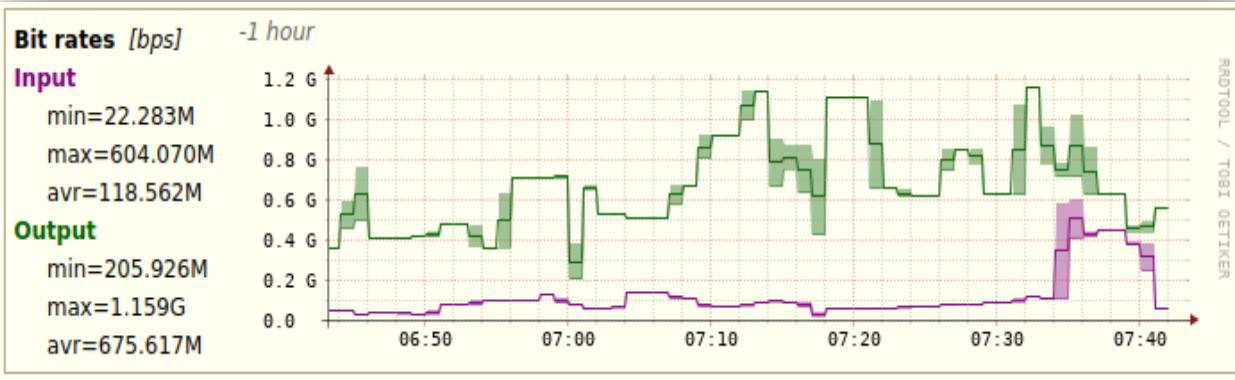


Sběr dat, nástroje

- 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

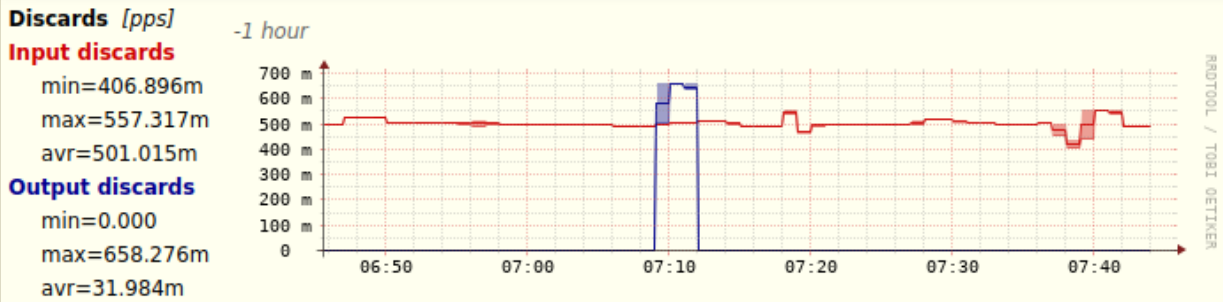
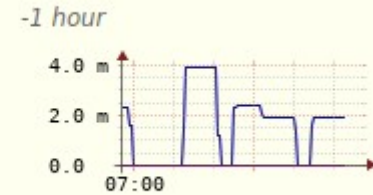
Interpretace dat ..bez ohledu na použitý nástroj

- správná interpretace ← znalost způsobu měření, znalost významu



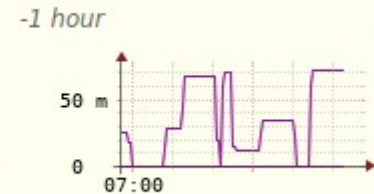
Ethernet errors [fps]

- alignment errors
- checksum errors
- frames too long
- SQE test errors
- internal MAC transmit errors
- internal MAC receive errors
- carrier sense errors



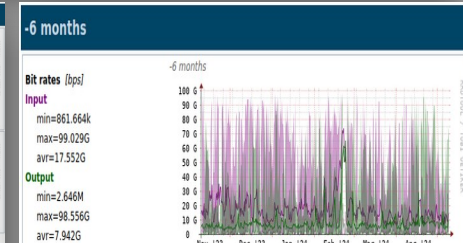
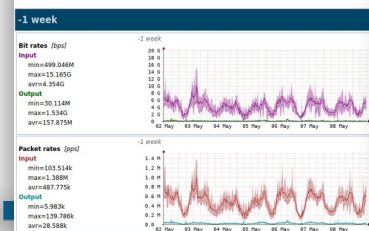
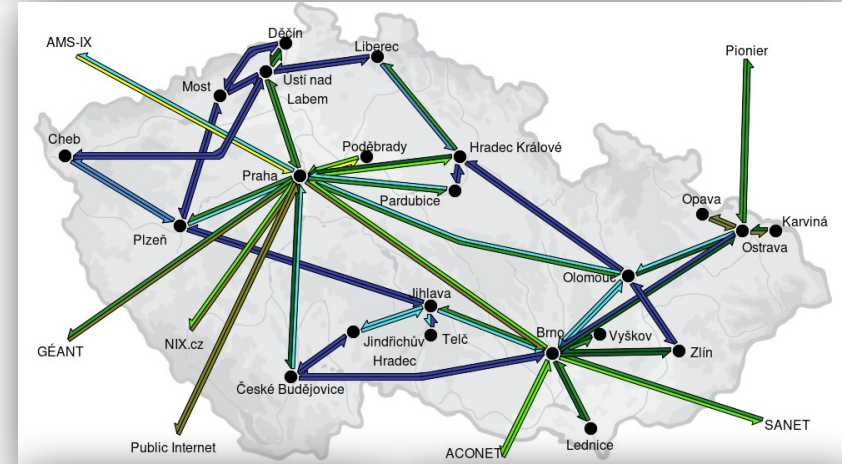
Ethernet errors [fps]

- alignment errors
- checksum errors
- frames too long
- SQE test errors
- internal MAC transmit errors
- internal MAC receive errors
- carrier sense errors



system 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



system G3

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

Reload/refresh

Object description filter ..?

cesnet3&NIX&[interface

case sensitive off On

apply as negative No Yes

apply as string

Time period

From -1 hour

To now

Others

Set tree template Full

Mark matching objects no, unmark all

Technological interface descriptions show

Color scheme khaki/yellow

CESNET3 -v

Praha

router, R -v

[Interfaces] -v

- Bundle-Ether104, #&73855572 NIX4 (CE Colo)
- Bundle-Ether104.10, #&65302478 NIX4 (CE Colo) - verejny peeri
- Bundle-Ether104.11, #&70718523 NIX4 (CE Colo) - FENIX, 2001:...
- HundredGigE0/0/0/8, #&81966685 NIX4 [TAP 50/50, 400G-XP slo

Praha

router, R -v

[Interfaces] -v

- Bundle-Ether102, #&57723227 NIX1 (CRa)
- Bundle-Ether102.10, #&11552296 NIX1 (CRa) - verejny peering,
- Bundle-Ether102.11, #&75025153 NIX1 (CRa) - FENIX, 2001:7f8:
- HundredGigE0/0/0/0, #&26458102 NIX1 (CRa) [BE102, TAP50/50

G3 system - user interface

version: 24.3, author: T

Compact UI Simple filtering Time period Navigation results Special checks Sessions Shared configurat

Reload/refresh

Object description filter ..?

gc .cesnet.cz

case sensitive off On

apply as negative No Yes

apply as string

Device filter based on object description filter ..?

Device filter

Time period

From -1 hour

To now

Others

Set tree template full

Mark matching objects no, unmark all

Technological interface descriptions show

Color scheme khaki/yellow

Show marked objects with the help of

- View (auto): 3. packet rates
- View (auto): 4. descriptions, states, bytes
- View (auto): 5. detailed analysis
- [HW] CPU utilization (CPU in last 1 min)
- [HW] DSP card utilization (Actual DSP)

CESNET2 -v

CESNET -v

server, gc cesnet.cz, FTAS-CESNET, gc ,195.113. -v

- [System]
- [IP]
- [TCP]
- [UDP]
- [ICMP]
- [SNMP]
- [Interfaces] -v
 - eth0, 2001:718:1:c: ,195.113.
 - eth1
 - lo, 0:0:0:0:0:0:1,127.0.0.1
- [HW] -v
 - *** HW overall information *** (structure, serial numbers, unclassified CPU)
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 0
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 1
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 2
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 3
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 4
 - GenuineIntel: Intel(R) Xeon(R) CPU E5-2660 v3 @ 2.60GHz, 5

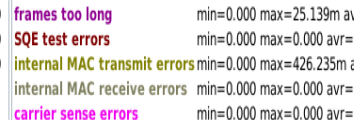
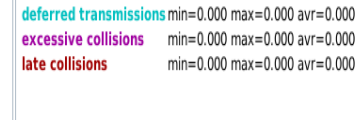
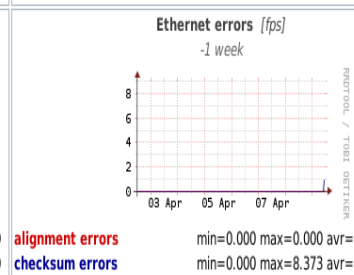
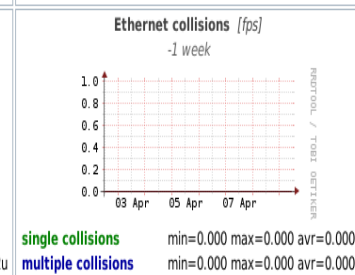
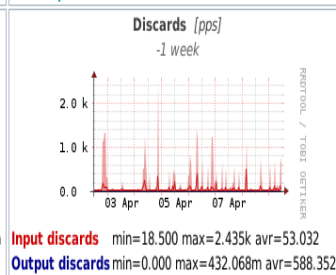
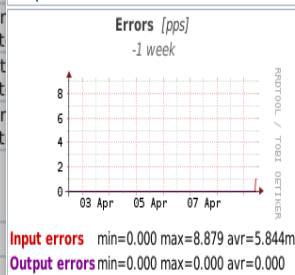
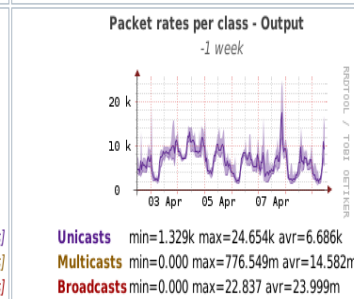
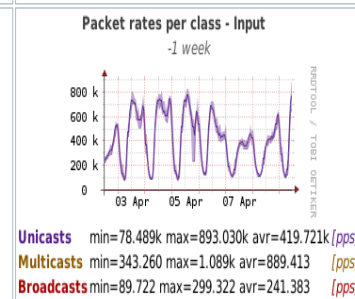
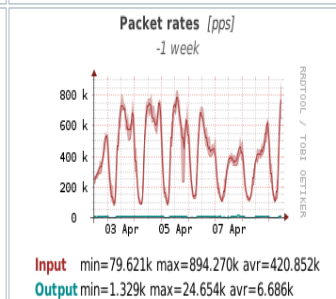
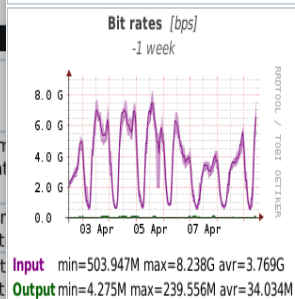
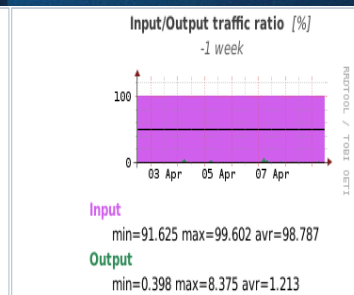
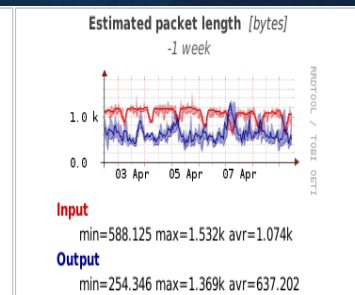
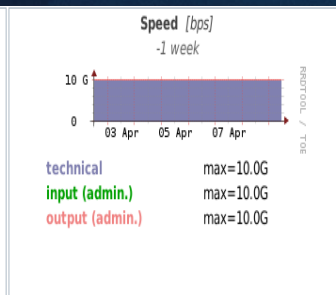
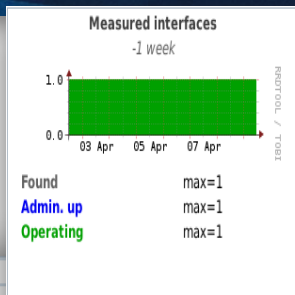
[+] CESNET3

- [+] Brno
- [+] Brno 1
 - [+] router, cesnet.cz, ...
 - [+] router, 3.cesnet.cz, ...
- [+] Brno 2
- [+] Ceske Budejovice

system 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:febf:597f 195.113.[REDACTED]
IPv6 address parameters [1]	2001:718:0:[REDACTED] inaccessible, manual, n fe80:0:0:0:8a1d:fcff:febf:597f preferred, stateful, stat fe80:0:0:0:8a1d:fcff:febf:597f stateless, unicast
IPv6 address parameters [2]	2001:718:0:[REDACTED] unicast, preferred, mar fe80:0:0:0:8a1d:fcff:febf:597f unicast, preferred, stat
IPv6 address parameters [3]	2001:718:0:[REDACTED] unicast, preferred, stat fe80:0:0:0:8a1d:fcff:febf:597f unicast, preferred, stat
IPv6 address parameters [4]	2001:718:0:[REDACTED] unicast, preferred, mar fe80:0:0:0:8a1d:fcff:febf:597f unicast, preferred, stat
IPv6 address parameters [5]	2001:718:0:[REDACTED] unicast, preferred, stat fe80:0:0:0:8a1d:fcff:febf:597f unicast, preferred, stat
IPv6 address parameters [6]	2001:718:0:[REDACTED] unicast, preferred, mar fe80:0:0:0:8a1d:fcff:febf:597f unicast, preferred, stat
IP network	2001:718:0:[REDACTED] fe80:0:0:0:8a1d:fcff:febf: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



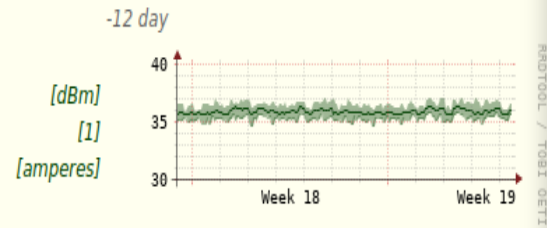
system G3

- ukázka UI - vizualizace

0/0-Hot Swap Fixed CS, sensor, Board Current 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 current	min=34.604 max=37.133 avr=35.891	[amperes]

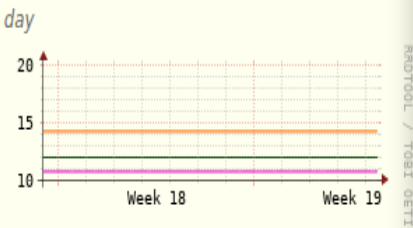


[View \(auto\): 5. detailed analysis](#)

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

Sensor with thresholds

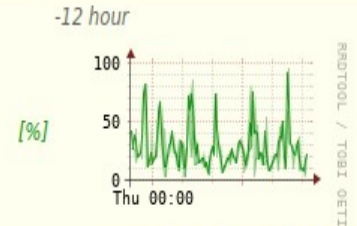
power/level	min=-nan max=-nan avr=-nan	[dBm]
true state	min=-nan max=-nan avr=-nan	[1]
electric potential DC	min=12.000 max=12.000 avr=12.000	[volts]
greater or equal critical threshold	min=14.4 max=14.4	
greater or equal major threshold	min=14.3 max=14.3	
greater or equal minor threshold	min=14.3 max=14.3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



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

CPU utilization

CPU current load min=3.000 max=95.000 avr=28.598

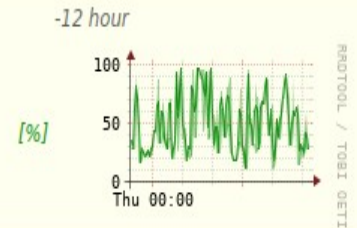


[View \(auto\): 5. detailed analysis](#)

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

CPU utilization

CPU current load min=11.000 max=97.000 avr=51.238

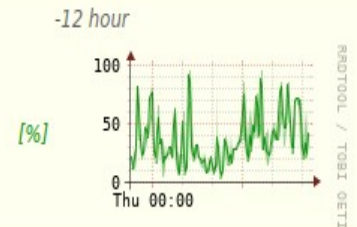


[View \(auto\): 5. detailed analysis](#)

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

CPU utilization

CPU current load min=4.000 max=96.000 avr=37.463



[View \(auto\): 5. detailed analysis](#)

system G3

- ukázka UI - vizualizace

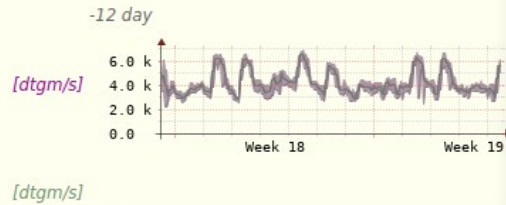
IP input traffic

Received datagrams

min=2.237k
max=6.933k
avr=4.227k

Locally delivered datagrams

min=2.237k
max=6.933k
avr=4.227k



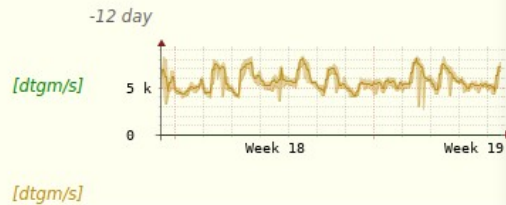
IP output traffic

Forwarded datagrams

min=0.000
max=0.000
avr=0.000

Local output requests

min=2.742k
max=8.517k
avr=5.760k



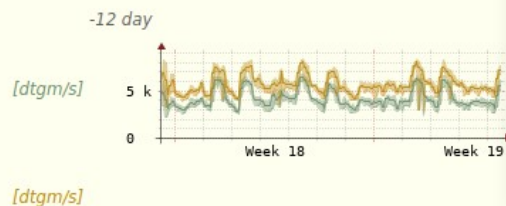
IP local traffic

Locally delivered datagrams

min=2.237k
max=6.933k
avr=4.227k

Local output requests

min=2.742k
max=8.517k
avr=5.760k



IP reassembling and fragmentation

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]

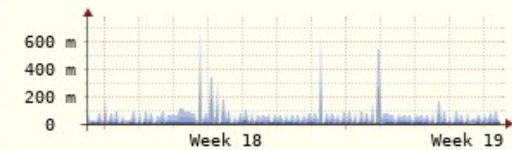
Fragments created

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]

-12 day



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]

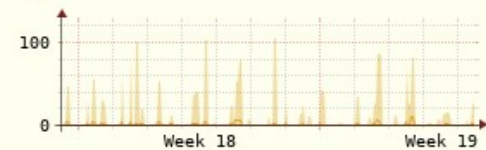
Output discards

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]

-12 day



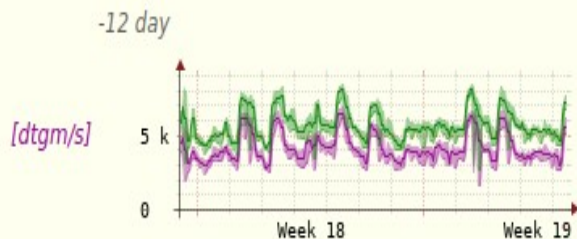
system G3

- ukázka UI - vizualizace

UDP traffic

Input datagrams

min=1.599k
max=6.921k
avr=4.220k



Output datagrams

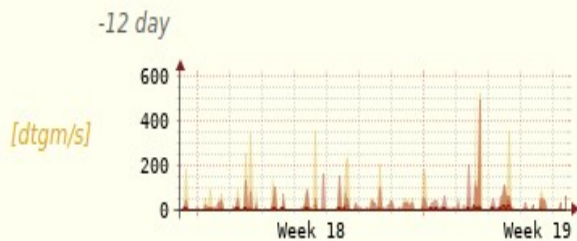
min=2.666k
max=8.514k
avr=5.759k



UDP problems

Invalid port

min=0.000
max=558.118
avr=2.340



Input errors

min=0.000
max=100.000

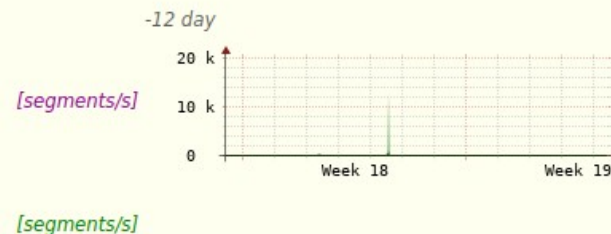
TCP traffic

Input segments

min=68.660m
max=1.072k
avr=1.311

Output segments

min=171.650m
max=13.155k
avr=4.575



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

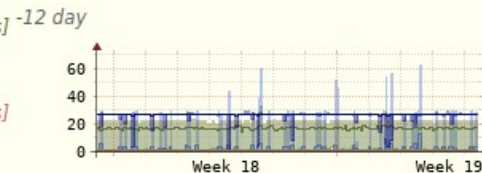
min=0.000
max=3.000
avr=1.534

[connections]

TCP connections ESTABLISHED or CLOSE-WAIT

min=2.000
max=30.000
avr=26.920

[connections]



TCP problems

Input errors

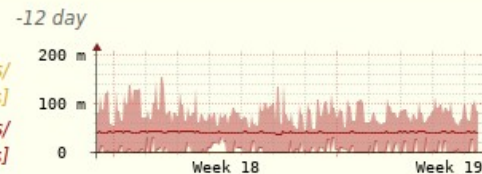
min=0.000 max=0.000
avr=0.000

[segments/s]

Segments containing RST flag sent

min=0.000 max=155.339m
avr=41.181m

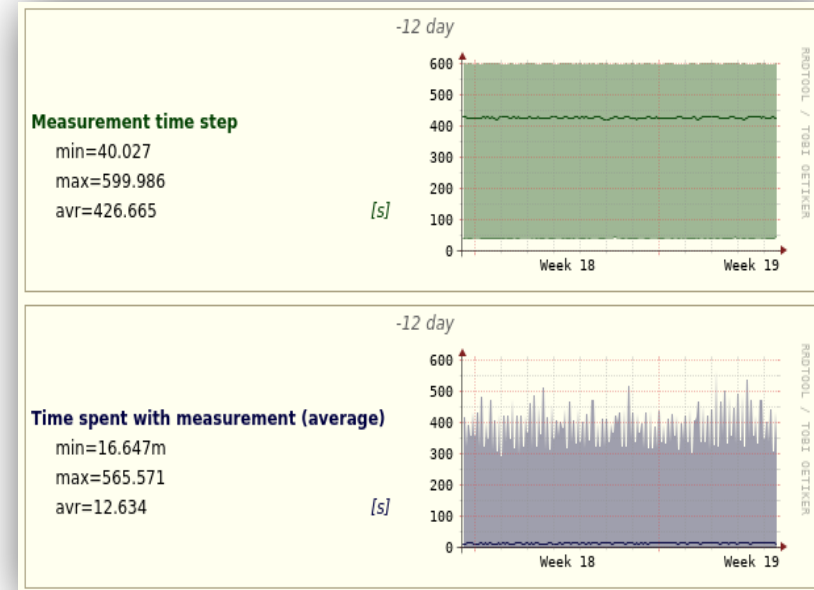
[segments/s]



system 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

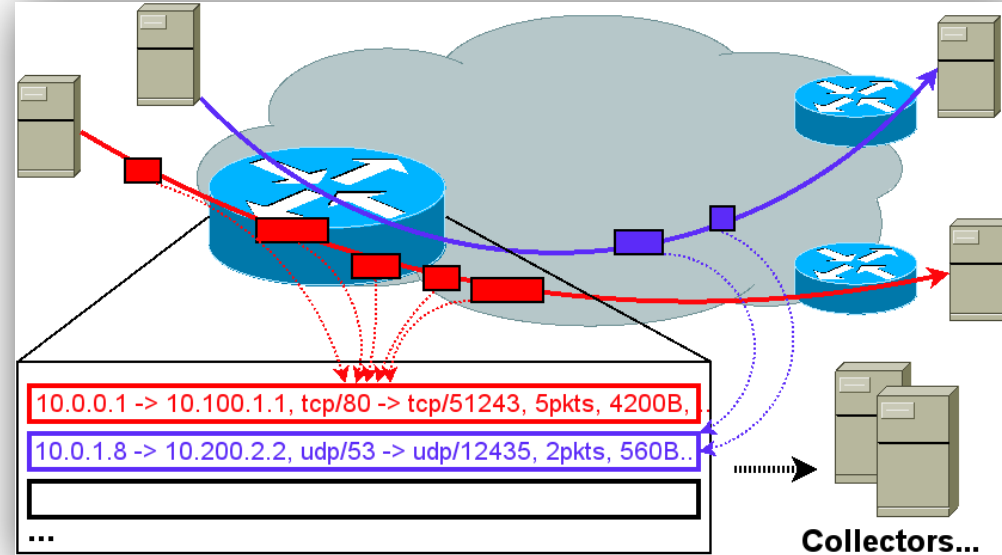


Monitoring provozu

- 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

CO+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
  
```

```

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	2001:718:x:9: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	2a00:1450:x:80e: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
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
362	171	0x60000000	0x60000000	AS32934	AS65002	24	16	00000000	push(8), ack(16)	195.x.x.x
128	213	0x60000000	0x60000000	AS65001	AS13074	16	24	00000000		195.x.x.x
213	128	0x60000000	0x60000000							
128	362	0x60000000	0x60000000							
362	157	0x60000000	0x60000000							

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 redukováný 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)

Src-IP	SNI	Min-TTL	Max-TTL	Flow-Start [CEST]	Flow-End [CEST]	Bytes-measured	Pkts-measured
157.240		58	58	24/05/13 09:35:43.158	24/05/13 09:40:40.936	190.295 MB	152.722 Kp
157.240	/socina.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
	-prod06-live.solocoo.tv	59	59	24/05/13 09:36:14.707	24/05/13 09:40:36.931	154.445 MB	109.045 Kp
		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	Forwarded									
ingress	Forwarded		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

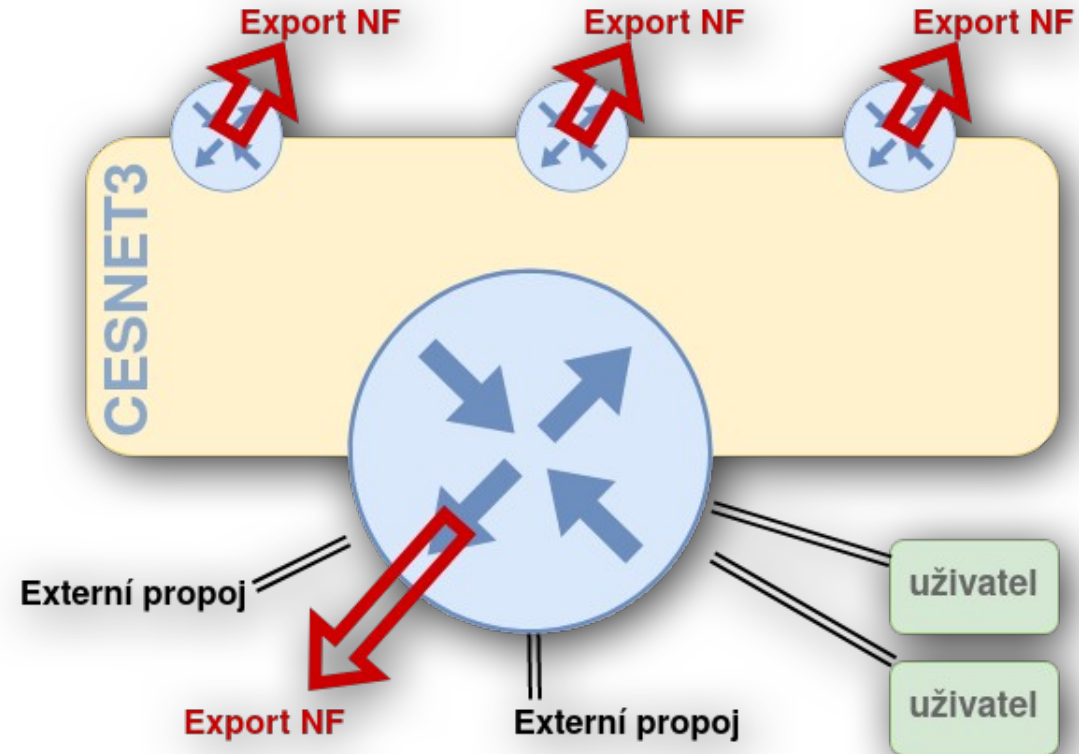
Důležité parametry

- **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



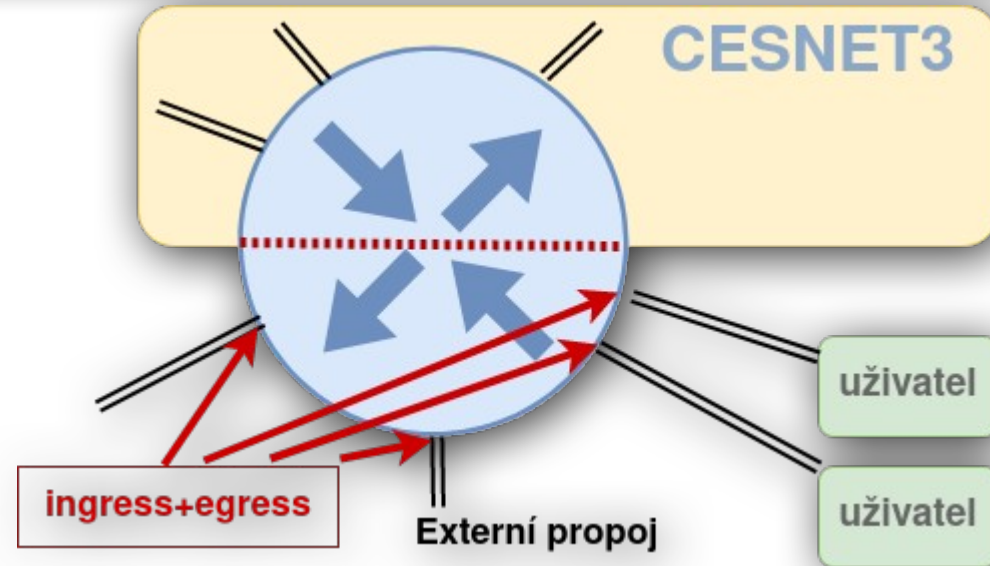
V e-infrastruktuře CESNET

- 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

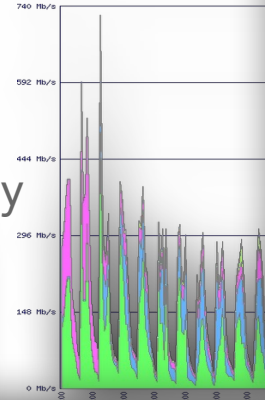
- nastavení zpracování NetFlow na páteřních směrovačích
 - ne rozhraní do jádra
 - všechna klientská a externí rozhraní
 - zpracování egress+ingress provozu
 - ingress - netflow z provozu, který vstupuje rozhraním do zařízení
 - egress - netflow z provozu, který vystupuje rozhraním ze zařízení



System 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

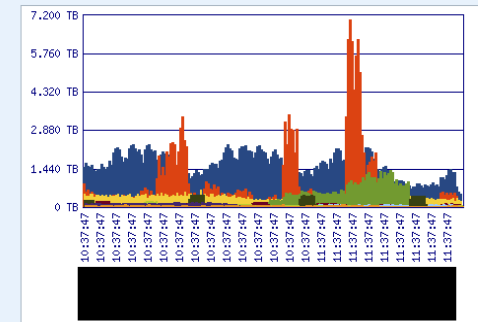
Flow-Direction	FWD-Status	Src-IP	Protocol	Src-Port	Src-Index	Dst-Index	Src/Prev-AS	TOS-flags	Bytes-estimated	Pkts-estimated	Flow-Cnt
1. ingress	Forwarded	77.75.11.1	tcp (6)	https (443)	156	49	AS43037	10101010	3.073 GB	2.844 Mp	26319
2. ingress	Forwarded	77.75.11.1	tcp (6)	https (443)	156	140	AS43037	00000010	693.980 MB	636.120 Kp	6119
3. ingress	Forwarded	2a02:5108:0:79:53	tcp (6)	https (443)	156	49	00000010	476.113 MB	444.960 Kp	4659	
4. ingress	Forwarded	2a02:5108:0:79:53	tcp (6)	https (443)	156	140	00000010	95.478 MB	88.600 Kp	929	
5. ingress	Forwarded	77.75.11.1	tcp (6)	https (443)	156	105	AS43037	00000010	73.180 MB	67.560 Kp	683
6. ingress	Forwarded	108.17.14.1	tcp (6)	https (443)	94742	49	AS15169	00000000	57.358 MB	72.440 Kp	492
7. ingress	Forwarded	108.17.14.1	tcp (6)	https (443)	94742	49	AS15169	00000000	34.728 MB	49.440 Kp	454



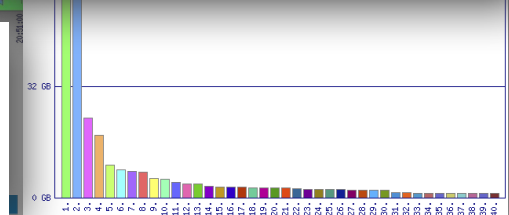
Bytes-estimated: sums/time steps, value per 3 hours, non-cumulative

Summary

In graph	708.443 TB	86.76%
Rest of results	108.094 TB	13.24%
Total	816.537 TB	100.00%

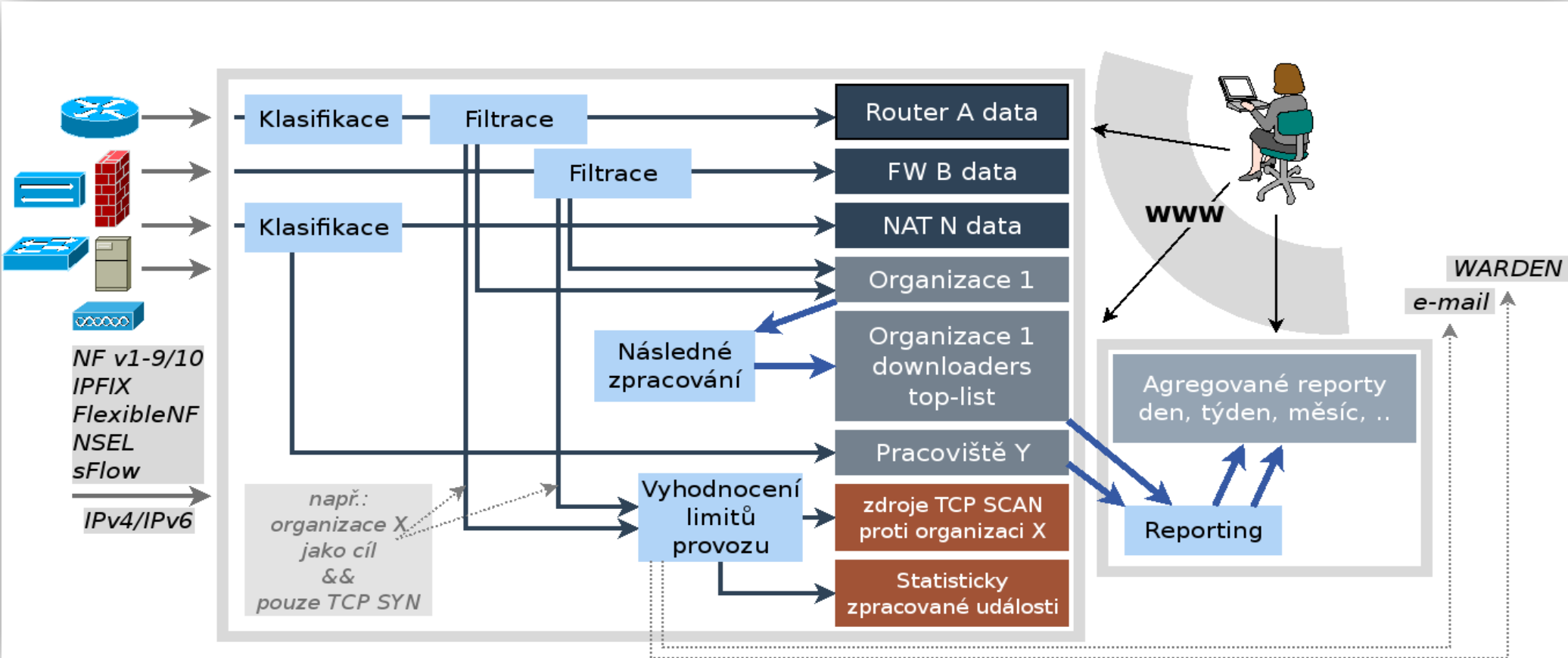


	Src-IP	Bytes-estimated	Pkts-estimated	Src-Object
1.	2001:718:1:...	309.152 TB ~ 37.861%	219.579 Gp ~ 25.478%	CESNET Praha
2.	2001:718:4:...	180.649 TB ~ 22.124%	138.761 Gp ~ 16.101%	CESNET2
3.	2001:718:ff:...	70.175 TB ~ 8.594%	48.476 Gp ~ 5.625%	CESNET2
4.	2001:718:ff:...	59.536 TB ~ 7.291%	43.356 Gp ~ 5.031%	CESNET2
5.	2001:718:80:...	20.546 TB ~ 2.516%	14.220 Gp ~ 1.650%	MU Brno
6.	2001:718:ff:...	16.920 TB ~ 2.072%	14.684 Gp ~ 1.704%	CESNET2
7.	2001:718:1:...	14.188 TB ~ 1.738%	10.295 Gp ~ 1.195%	CESNET DC/VI
8.	2001:718:1:...	13.842 TB ~ 1.695%	9.852 Gp ~ 1.143%	CESNET Praha
9.	2001:718:ff:...	11.905 TB ~ 1.458%	11.579 Gp ~ 1.344%	CESNET2
10.	2001:718:1:...	11.530 TB ~ 1.412%	58.568 Gp ~ 6.796%	UK Praha



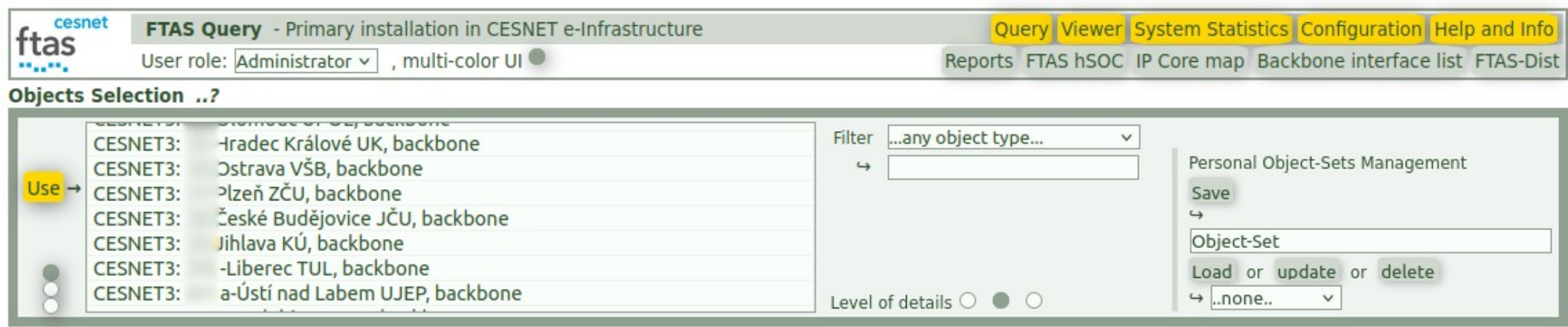
```
# Src-IP;Src-GeoIP;Bytes-estimated;Bytes-estimated-Percent;Pkts-estimated;Pkts-estimated-Percent;Flow-Cnt;Flow-Cnt-Percent;Detector-Type;Detector-Name
# src_ip;src_ip_cc;statist_octets;statist_octets_percent;statist_pkts;statist_pkts_percent;flowcnt;flowcnt_percent;detector_type;detector
185.22.11.1;666308800;0.0800714469973045;16657720;0.0802009849319872;416443;0.0801883512289643;Src-IP;TCP SYN against internal IP address ranges, sources
80.82.11.1;589342400;0.0708222655094218;14733560;0.0709368403091497;368339;0.0709256659454607;Src-IP;TCP SYN against internal IP address ranges, sources
5.188.11.1;539766400;0.0648646343685178;13494160;0.0649695710355213;337354;0.0649593366691144;Src-IP;TCP SYN against internal IP address ranges, sources
5.8.18.11.1;431857600;0.0518970527310807;10796440;0.0519810107120965;269911;0.0519728223755976;Src-IP;TCP SYN against internal IP address ranges, sources
80.82.11.1;412067200;0.0495188071418653;10301680;0.0495989176462417;257542;0.0495911045502264;Src-IP;TCP SYN against internal IP address ranges, sources
5.8.18.11.1;399057600;0.0479554216712604;9976440;0.0480330029628829;249411;0.0480254365384151;Src-IP;TCP SYN against internal IP address ranges, sources
5.188.11.1;390915200;0.0469769357949958;9772880;0.0470529341123587;244322;0.0470455220737604;Src-IP;TCP SYN against internal IP address ranges, sources
```


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



System FTAS

- ukázky UI
- výber zdrojů dat



The screenshot shows the FTAS Query web interface. The top navigation bar includes links for Query, Viewer, System Statistics, Configuration, and Help and Info. The user role is set to Administrator, and the multi-color UI is selected. The main content area is titled "Objects Selection ..?" and displays a list of network objects with their locations and roles. A "Use" button is visible next to the first object. To the right, there is a filter dropdown set to "...any object type...", a search input field, and a "Level of details" section with three radio buttons. On the far right, the "Personal Object-Sets Management" section includes a "Save" button, an "Object-Set" input field, and "Load or update or delete" options with a dropdown set to "...none..".

Object ID	Location	Role
CESNET3: 1	Hradec Králové	backbone
CESNET3: 2	Ostrava VŠB	backbone
CESNET3: 3	Plzeň ZČU	backbone
CESNET3: 4	České Budějovice JČU	backbone
CESNET3: 5	Jihlava KÚ	backbone
CESNET3: 6	Liberec TUL	backbone
CESNET3: 7	a-Ústí nad Labem UJEP	backbone

System FTAS

- ukázky UI
- vyhledávání

Objects Selection ..?

Flow Data Source	
CESNET3: Praha	
CESNET3: P-Prah	
CESNET3: P-Prah	
CESNET3: Brno MUNI, backbone, border router	
CESNET3: Olomouc UPOL, backbone	
CESNET3: Hradec Králové UK, backbone	
CESNET3: Ostrava VŠB, backbone	

Filter:

Personal Object-Sets Management
 Save

 Load or update or delete

Query Parameters ..?

Fields to store in results ..?

Flow Src/Dst Fields

- Src-IP *
- Src-Port *
- Src-ifIndex *
- Ingress-VRFLID *
- Src/Prev-AS *
- Src-Bitmask *
- Dst-IP *
- Dst-Port *
- Dst-ifIndex *
- Egress-VRFLID *
- Dst/Next-AS *
- Dst-Bitmask *

Flow Common Fields

- Flow-Direction *
- FWD-Status *
- Flow-Labelv6 *
- IP-Version *
- Protocol *
- TOS-flags
- TCP-flags
- Nexthop *
- Min-TTL
- Max-TTL
- Flow Data Source *

Time, Value and Count Fields

- Flow-Start
- Flow-End
- Bytes-measured
- Bytes-estimated
- Pkts-measured
- Pkts-estimated
- Flow-Cnt

Fields Query Condition - Simple Form ..?

...you can switch to 'generic' condition form

Query traffic (in form below) from Source to Destination bidirectional from Destination to Source

Source	relation	Destination
IP address: <input type="text" value="www.seznam.cz"/>	and v	<input type="text"/>
Service Port: <input type="text" value="80,443"/>	and v	<input type="text"/>
AS Number: <input type="text"/>	and v	<input type="text"/>
Interface Index: <input type="text"/>	and v	<input type="text"/>
VRFLID: <input type="text"/>	and v	<input type="text"/>

Protocol

TCP-flags

TOS-flags

Flow-Direction

FWD-Status

IP-Version:

Flow-Labelv6:

Transferred through:

Query Condition Management

Time Parameters ..?

...advanced ...check time values

Flow last>= GMT time

Flow first<=

cut flows at time interval border ..?
sub-aggregation period → ..?
data table sampling → ..?

Aggregation → ..? ...when set to 'yes', then 'group by' clause is constructed from selected (* labeled) fields and applied on each source data table + result of aggregation can be ordered by , limited up to records/table before storing to final results..

Query Processing ..?

Run New Query → Max. duration Max. count

without graphs

Run on background

Query name (when 'Run New Query')



System FTAS

- ukázky UI
- vyhledávání

Objects Selection ..?

Flow Data Source	Filter
<input checked="" type="radio"/> Use → CESNET3: Praha CESNET3: -Prah. CESNET3: +Prah. CESNET3: Brno MUNI, backbone, border router CESNET3: Olomouc UPOL, backbone CESNET3: Hradec Králové UK, backbone CESNET3: Octava VŠB, backbone	...any object type... <input type="text" value="cesnet3"/>

Personal Object-Sets Management

Save

Object-Set

Load or update or delete

↔ ..none..

Level of details ● ○ ○

Query Parameters ..?

Fields to store in results ..?

Flow Src/Dst Fields

<input type="radio"/> Src-IP *	<input type="radio"/> Dst-IP *
<input type="radio"/> Src-Port *	<input type="radio"/> Dst-Port *
<input type="radio"/> Src-ifIndex *	<input type="radio"/> Dst-ifIndex *
<input type="radio"/> Ingress-VRFID *	<input type="radio"/> Egress-VRFID *
<input type="radio"/> Src/Prev-AS *	<input type="radio"/> Dst/Next-AS *
<input type="radio"/> Src-Bitmask *	<input type="radio"/> Dst-Bitmask *

Flow Common Fields

<input type="radio"/> Flow-Direction *	<input type="radio"/> TCP-flags
<input type="radio"/> FWD-Status *	<input type="radio"/> Nexthop *
<input type="radio"/> Flow-Labelv6 *	<input type="radio"/> Min-TTL
<input type="radio"/> IP-Version *	<input type="radio"/> Max-TTL
<input type="radio"/> Protocol *	<input type="radio"/> Flow Data Source *
<input type="radio"/> TOS-flags	

Time, Value and Count Fields

<input type="radio"/> Flow-Start	<input type="radio"/> Pkts-measured
<input type="radio"/> Flow-End	<input type="radio"/> Pkts-estimated
<input type="radio"/> Bytes-measured	<input checked="" type="radio"/> Flow-Cnt
<input type="radio"/> Bytes-estimated	

Query Condition - Generic Form ..?

...you can switch to 'simple' condition form

Conditions for 'Source', 'Destination' and 'Common' flow fields ('WHERE clause'). ..?

```
(src_ip=www.seznam.cz and src_port=80,443 and proto=6) or (dst_ip=www.seznam.cz and dst_port=80,443 and proto=6)
```

Conditions for value and count fields ('HAVING clause'). ..?

Query Condition Management

Time Parameters ..?

...advanced ● ...check time values ○

cut flows at time interval border ..?

sub-aggregation period → auto ..?

data table sampling → 1 ..?

Flow last >= -10 minutes
 Flow first <= now

GMT time

Aggregation → no ..?

...when set to 'yes', then 'group by' clause is constructed from selected (* labeled) fields and applied on each source data table + result of aggregation can be ordered by none asc., limited up to records/table before storing to final results..

Query Processing ..?

Run New Query →

Max. duration 30 seconds

Max. count 20000 records

without graphs

Run on background

Notify to (e-mail)

Query name (when 'Run New Query')

System FTAS

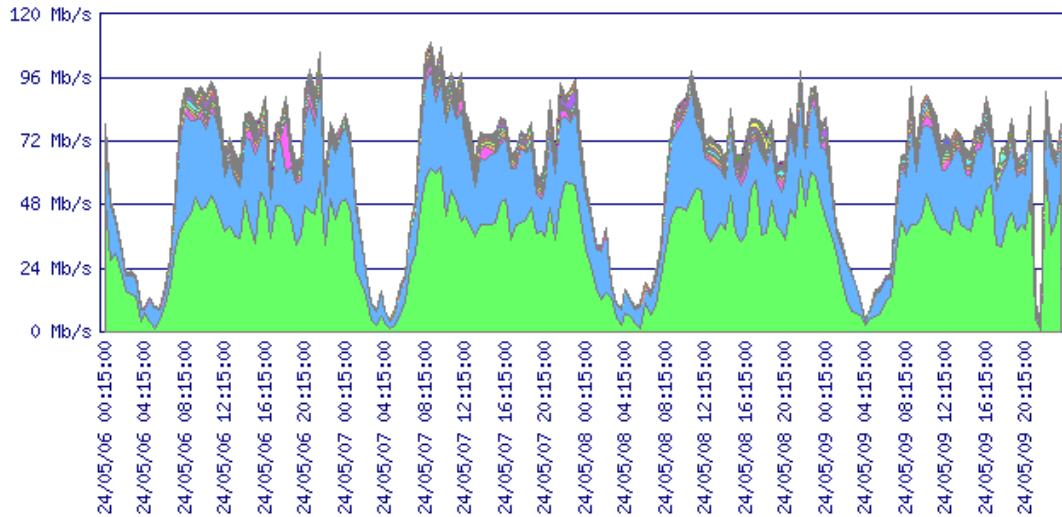
- ukázky UI - vizualizace

Flow-Direction	FWD-Status	IP-Version	Src-IP	Dst-IP	Protocol	Src-Port	Dst-Port	Src-ifIndex	Dst-ifIndex	Ingress-VRID	Egress-VRID
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

System FTAS

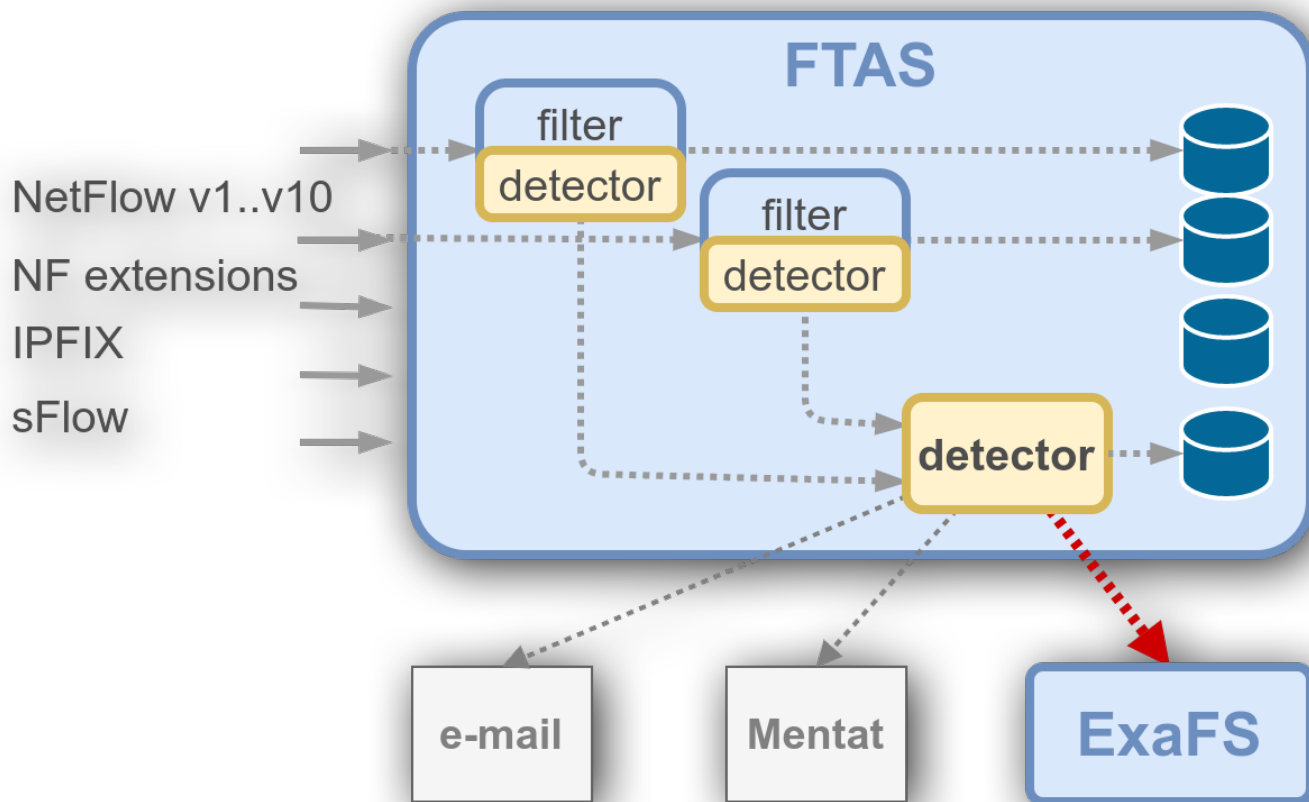
- ukázky UI - vizualizace



0 >	Flow-Direction	FWD-Status	IP-Version	Src-IP	Protocol	Src-Port	Bytes-estimated	Dst-IP-Cnt
1 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	udp (17)	https (443)	1.498 TB	83
2 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	udp (17)	https (443)	888.931 GB	119
3 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	tcp (6)	https (443)	64.660 GB	123
4 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	udp (17)	https (443)	39.866 GB	27
5 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	udp (17)	https (443)	30.382 GB	97
6 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	tcp (6)	https (443)	29.187 GB	95
7 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	udp (17)	https (443)	27.221 GB	36
8 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	tcp (6)	https (443)	23.407 GB	115
9 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	udp (17)	3478	16.469 GB	15
0 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	tcp (6)	https (443)	15.026 GB	34
1 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	tcp (6)	https (443)	12.838 GB	91
2 >	egress	Forwarded	4	157.240.30.42 www.facebook.com	udp (17)	https (443)	11.756 GB	78
13 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	udp (17)	3478	8.565 GB	12
14 >	egress	Forwarded	4	157.240.30.42 instagram-photos-01-prg1.facebook.com	udp (17)	3478	6.127 GB	13
15 >	egress	Forwarded	4	157.240.30.42 edge-star-mini-shv-01-prg1.facebook.com	udp (17)	https (443)	6.118 GB	116

System FTAS – detekční prvky

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



ExaFS

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

The screenshot shows the ExaFS web interface. At the top, there are navigation links: "Add IPv4", "Add IPv6", "Add RTBH", and "API Key". The user is identified as "Petr Adamec".

Active IPv4 rules

Summary: IPv4 (43) | IPv6 (0) | RTBH (0)

Active IPv4 rules that you can modify

Source addr.	S port	Dest. addr.	D port	Proto	Packet len	Expires	Action	Flags	User	Edit
17.242/32				icmp		2024/04/02 19:20	QoS 0.1 Mbps			[Refresh] [Delete] [Info]

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
2.0.0/24		18.0.0/16	22	tcp		2042/02/03 22:20	Discard			[Info]
		18.97.163/32		all		2026/10/17 12:10	Discard			[Info]
						2025/08/18 10:00	QoS 10 Mbps			[Info]
						2025/08/18 10:00	QoS 10 Mbps			[Info]

New IPv4 rule form:

- Source address: []
- Source mask (bits): []
- Protocol: TCP
- Destination address: []
- Destination mask (bits): []
- Fragment: []
- Source port(s): []
- Destination port(s): []
- Packet length: []
- Action: [select action]
- Expiration date: 12.03.2024 13.44

New RTBH rule form:

- IPv4 address: 192.168.0.1
- IPv4 mask (bits): []
- Community: [select community]
- Expiration date: 12.03.2024 13.13
- Comments: Test

ExaFS

RTBH

BGP FlowSpec

externí čištění

"přesměrování"

DDoS Protector

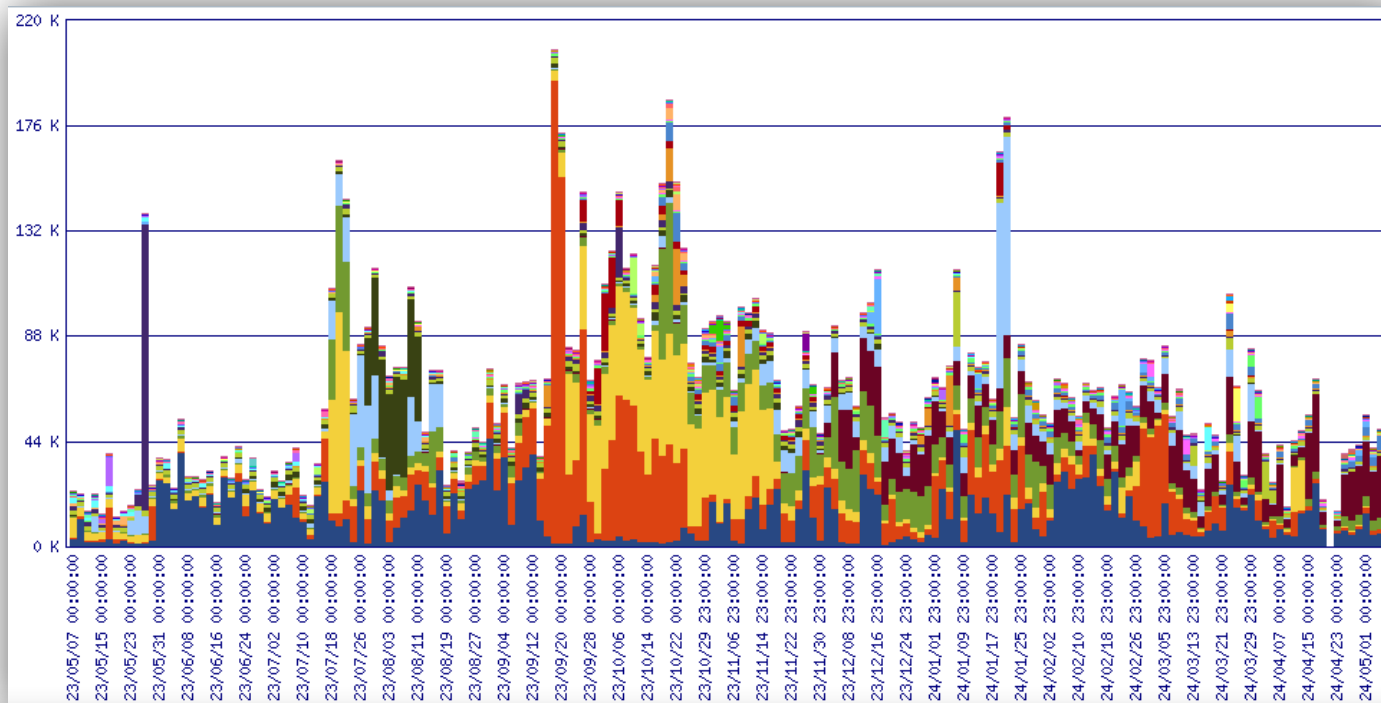
FTAS → obranné role

- 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



System FTAS

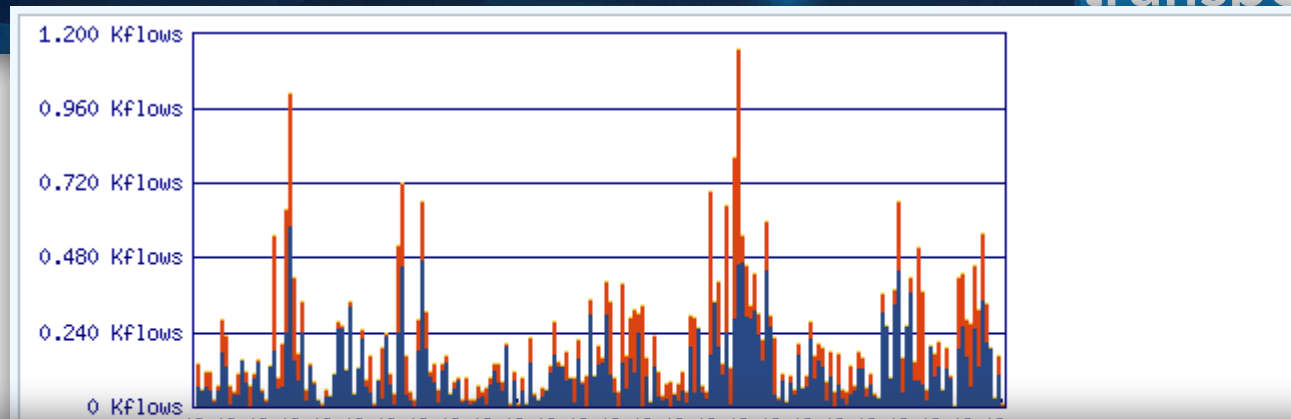
- ukázky UI – vizualizace
- celá komunita
- roční průběh agregátů detekovaných událostí za 2 dny – ve špičkách více než 2/s



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

System FTAS

- ukázky UI – vizualizace
- specifický detektor (ČZU)



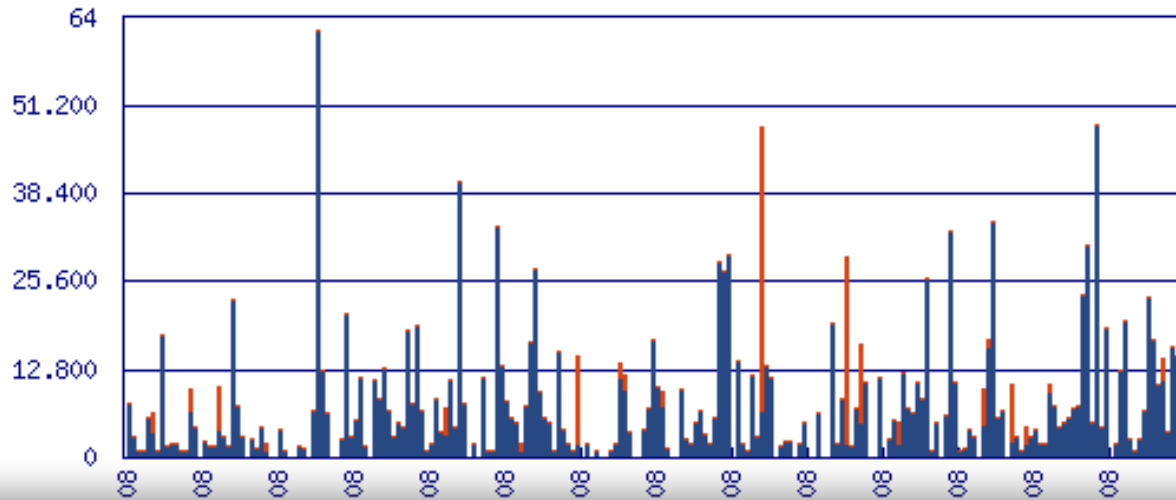
Flow-Cnt: sums/time steps, 24/05/06 10:47:16-24/05/13 10:47:16, value per 50 minutes, cumulative

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

System 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.

