Benefity a úskalí plošného souvislého sledování IP provozu na bázi toků při řešení bezpečnostních hlášení

Tomáš Košňar

CESNET z.s.p.o.

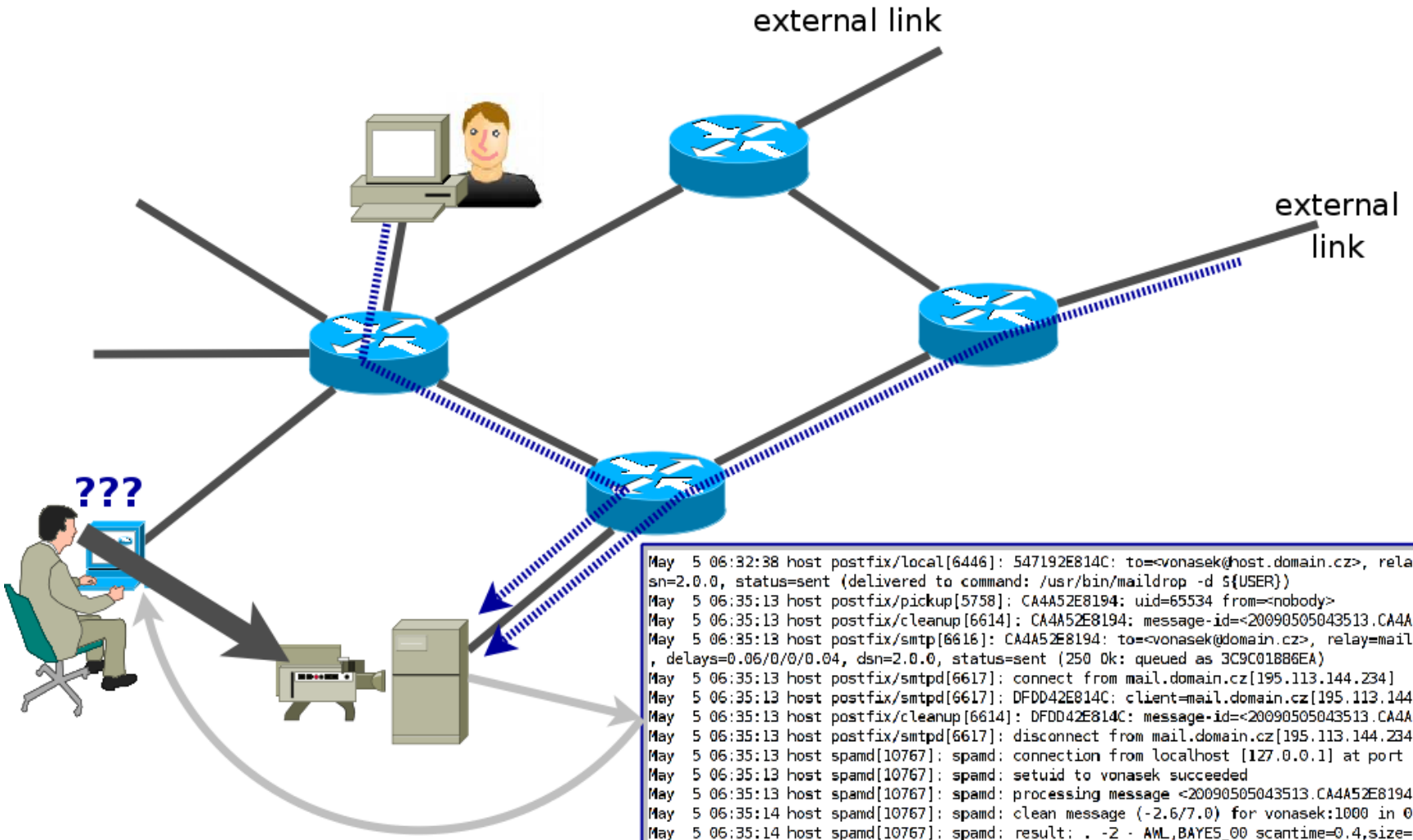
kosnar@cesnet.cz

Obsah

- požadavky plynoucí z bezpečnostních hlášení
- provozní informace na bázi IP toků
- zdroje provozních záznamů na bázi IP toků
- objemy provozních záznamů na bázi IP toků
- zpracování provozních záznamů na bázi IP toků
- zhodnocení

Požadavky plynoucí z bezpečnostních hlášení

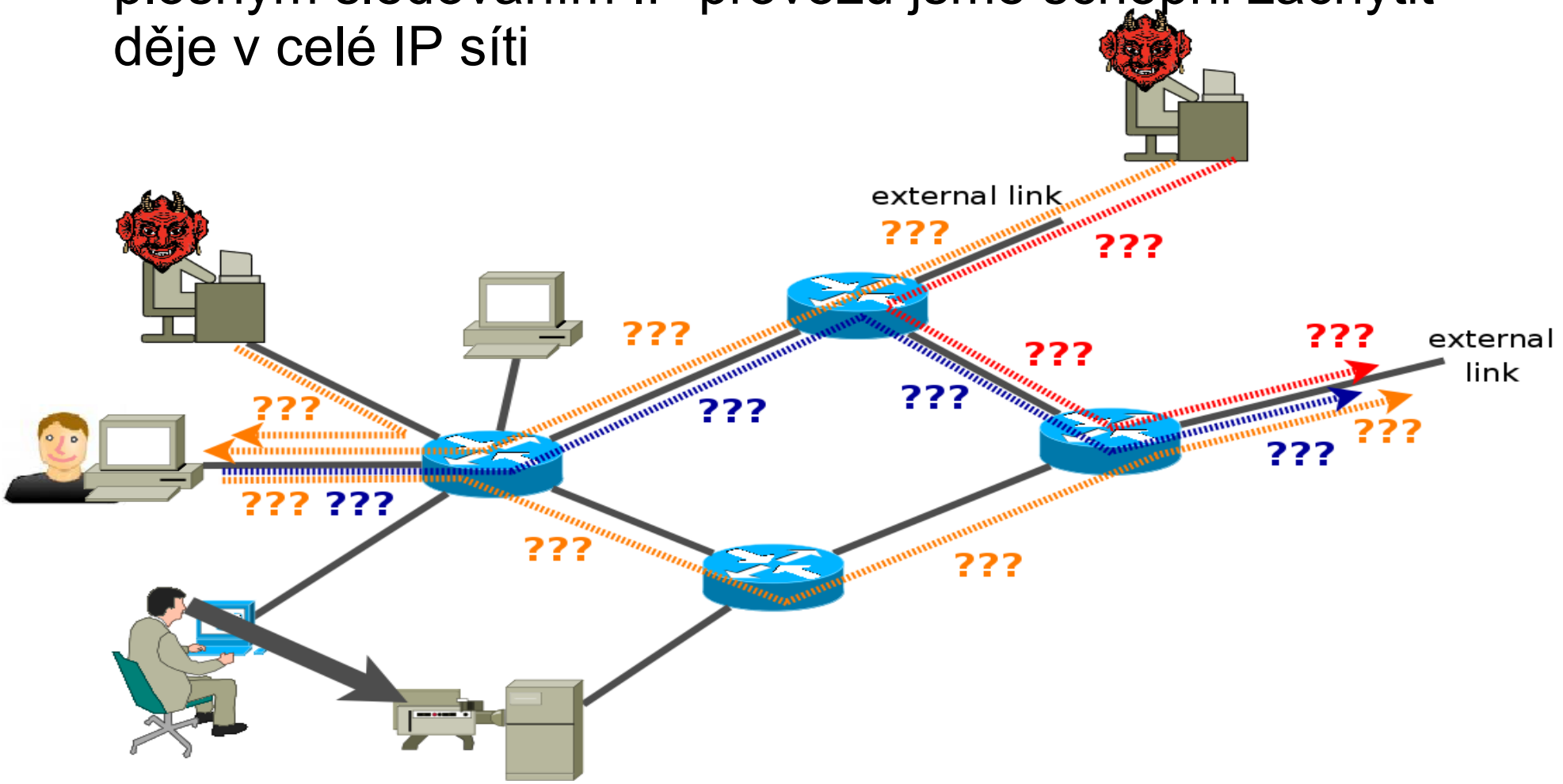
- „tradiční způsob“ ověřování možných anomálií




```
May  5 06:32:38 host postfix/local[6446]: 547192E814C: to=<vonasek@host.domain.cz>, relay=local, delay=5.7, delays=0.03/0
sn=2.0.0, status=sent (delivered to command: /usr/bin/maildrop -d ${USER})
May  5 06:35:13 host postfix/pickup[5758]: CA4A52E8194: uid=65534 from=<nobody>
May  5 06:35:13 host postfix/cleanup[6614]: CA4A52E8194: message-id=<20090505043513.CA4A52E8194@host.domain.cz>
May  5 06:35:13 host postfix/smtp[6616]: CA4A52E8194: to=<vonasek@domain.cz>, relay=mail.domain.cz[195.113.144.234]:25, d
, delays=0.06/0/0/0.04, dsn=2.0.0, status=sent (250 Ok: queued as 3C9C018B6EA)
May  5 06:35:13 host postfix/smtpd[6617]: connect from mail.domain.cz[195.113.144.234]
May  5 06:35:13 host postfix/smtpd[6617]: DFDD42E814C: client=mail.domain.cz[195.113.144.234]
May  5 06:35:13 host postfix/cleanup[6614]: DFDD42E814C: message-id=<20090505043513.CA4A52E8194@host.domain.cz>
May  5 06:35:13 host postfix/smtpd[6617]: disconnect from mail.domain.cz[195.113.144.234]
May  5 06:35:13 host spamd[10767]: spamd: connection from localhost [127.0.0.1] at port 42172
May  5 06:35:13 host spamd[10767]: spamd: setuid to vonasek succeeded
May  5 06:35:13 host spamd[10767]: spamd: processing message <20090505043513.CA4A52E8194@host.domain.cz> for vonasek:1000
May  5 06:35:14 host spamd[10767]: spamd: clean message (-2.6/7.0) for vonasek:1000 in 0.4 seconds, 1240 bytes.
May  5 06:35:14 host spamd[10767]: spamd: result: . -2 - AWL,BAYES_00 scantime=0.4,size=1240,user=vonasek,uid=1000,requir
7.0,rhost=localhost,raddr=127.0.0.1,rport=42172,mid=<20090505043513.CA4A52E8194@host.domain.cz>,bayes=0.000000,autolearn=
May  5 06:35:14 host spamd[5603]: prefork: child states: II
```

Požadavky plynoucí z bezpečnostních hlášení

- „tradiční způsob“ ověřování možných anomálií postihne sice přesně (není-li uzel kompromitován), ale pouze velmi malou podmnožinu událostí - *co „nedoteče“ k místu pozorování, to „neexistuje“*
- plošným sledováním IP provozu jsme schopni zachytit děje v celé IP síti



Požadavky plynoucí z bezpečnostních hlášení

- co je požadováno ?

  A. potvrdit nebo vyvrátit fakta specifikovaná v bezpečnostním hlášení v míře, v jaké je to na úrovni informací o provozu možné

  - hlášení zpravidla obsahuje přesné vymezení a typ události
    - porušení užívacích práv (konkrétní zdokumentovaný příklad)
    - systematické agresivní útoky (DoS, DDoS, „network scanninng“, slovníkové útoky, TCP SYN flooding..)
    - cíle podsunuté v rámci phishingu
    - ...

Požadavky plynoucí z bezpečnostních hlášení

- například verifikace - plošný ms-sql-srv scan ve vymezeném období z dané IP adresy...

o	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Flow-Start	Flow-End	Src-Port	Dst-Port	Protocol
1.	209.152.44.9	147.32.15.193	1.000 p	46.000 B	09/05/12 11:04:43.117	09/05/12 11:04:43.117	7815	ms-sql-s (1433)	tcp (6)
2.	209.152.44.9	147.32.12.173	1.000 p	46.000 B	09/05/12 11:04:43.117	09/05/12 11:04:43.117	5345	ms-sql-s (1433)	tcp (6)
3.	209.152.44.9	147.32.14.228	1.000 p	46.000 B	09/05/12 11:04:43.117	09/05/12 11:04:43.117	33107	ms-sql-s (1433)	tcp (6)
4.	209.152.44.9	147.32.12.4	1.000 p	46.000 B	09/05/12 11:04:43.118	09/05/12 11:04:43.118	5175	ms-sql-s (1433)	tcp (6)
5.	209.152.44.9	147.32.13.5	1.000 p	46.000 B	09/05/12 11:04:43.145	09/05/12 11:04:43.145	5430	ms-sql-s (1433)	tcp (6)
6.	209.152.44.9	147.32.13.67	1.000 p	46.000 B	09/05/12 11:04:43.145	09/05/12 11:04:43.145	5496	ms-sql-s (1433)	tcp (6)
7.	209.152.44.9	147.32.13.17	1.000 p	46.000 B	09/05/12 11:04:46.320	09/05/12 11:04:46.320	5442	ms-sql-s (1433)	tcp (6)
8.	209.152.44.9	147.32.13.93	1.000 p	46.000 B	09/05/12 11:04:46.320	09/05/12 11:04:46.320	5930	ms-sql-s (1433)	tcp (6)
9.	209.152.44.9	147.32.12.206	1.000 p	46.000 B	09/05/12 11:04:46.320	09/05/12 11:04:46.320	5375	ms-sql-s (1433)	tcp (6)
10.	209.152.44.9	147.32.12.198	1.000 p	46.000 B	09/05/12 11:04:46.320	09/05/12 11:04:46.320	5368	ms-sql-s (1433)	tcp (6)
11.	209.152.44.9	147.32.12.100	1.000 p	46.000 B	09/05/12 11:04:46.321	09/05/12 11:04:46.321	5271	ms-sql-s (1433)	tcp (6)
12.	209.152.44.9	147.32.14.120	1.000 p	46.000 B	09/05/12 11:04:46.336	09/05/12 11:04:46.336	24605	ms-sql-s (1433)	tcp (6)
13.	209.152.44.9	147.32.14.217	1.000 p	46.000 B	09/05/12 11:04:46.337	09/05/12 11:04:46.337	34424	ms-sql-s (1433)	tcp (6)
14.	209.152.44.9	147.32.15.55	1.000 p	46.000 B	09/05/12 11:04:47.798	09/05/12 11:04:47.798	35870	ms-sql-s (1433)	tcp (6)
15.	209.152.44.9	147.32.13.252	1.000 p	46.000 B	09/05/12 11:04:47.798	09/05/12 11:04:47.798	22216	ms-sql-s (1433)	tcp (6)
16.	209.152.44.9	147.32.12.184	1.000 p	46.000 B	09/05/12 11:04:47.799	09/05/12 11:04:47.799	hostmon (5355)	ms-sql-s (1433)	tcp (6)
17.	209.152.44.9	147.32.15.195	1.000 p	46.000 B	09/05/12 11:04:47.799	09/05/12 11:04:47.799	8218	ms-sql-s (1433)	tcp (6)
18.	209.152.44.9	147.32.14.108	1.000 p	46.000 B	09/05/12 11:04:47.799	09/05/12 11:04:47.799	20147	ms-sql-s (1433)	tcp (6)
19.	209.152.44.9	147.32.12.243	1.000 p	46.000 B	09/05/12 11:04:47.799	09/05/12 11:04:47.799	5414	ms-sql-s (1433)	tcp (6)
20.	209.152.44.9	147.32.13.217	1.000 p	46.000 B	09/05/12 11:04:47.800	09/05/12 11:04:47.800	17986	ms-sql-s (1433)	tcp (6)
21.	209.152.44.9	147.32.12.233	1.000 p	46.000 B	09/05/12 11:04:47.800	09/05/12 11:04:47.800	5405	ms-sql-s (1433)	tcp (6)
22.	209.152.44.9	147.32.12.124	1.000 p	46.000 B	09/05/12 11:04:47.800	09/05/12 11:04:47.800	5294	ms-sql-s (1433)	tcp (6)
23.	209.152.44.9	147.32.12.98	1.000 p	46.000 B	09/05/12 11:04:50.674	09/05/12 11:04:50.674	5267	ms-sql-s (1433)	tcp (6)
24.	209.152.44.9	147.32.13.20	1.000 p	46.000 B	09/05/12 11:04:50.693	09/05/12 11:04:50.693	5444	ms-sql-s (1433)	tcp (6)
25.	209.152.44.9	147.32.15.64	1.000 p	46.000 B	09/05/12 11:04:50.693	09/05/12 11:04:50.693	37644	ms-sql-s (1433)	tcp (6)
26.	209.152.44.9	147.32.12.147	1.000 p	46.000 B	09/05/12 11:04:50.910	09/05/12 11:04:50.910	5318	ms-sql-s (1433)	tcp (6)
27.	209.152.44.9	147.32.12.49	1.000 p	46.000 B	09/05/12 11:04:50.925	09/05/12 11:04:50.925	5220	ms-sql-s (1433)	tcp (6)
28.	209.152.44.9	147.32.13.7	1.000 p	46.000 B	09/05/12 11:04:50.925	09/05/12 11:04:50.925	postgresql (5432)	ms-sql-s (1433)	tcp (6)
29.	209.152.44.9	147.32.13.134	1.000 p	46.000 B	09/05/12 11:04:56.417	09/05/12 11:04:56.417	7996	ms-sql-s (1433)	tcp (6)
30.	209.152.44.9	147.32.15.53	1.000 p	46.000 B	09/05/12 11:04:58.051	09/05/12 11:04:58.051	35914	ms-sql-s (1433)	tcp (6)

Požadavky plynoucí z bezpečnostních hlášení

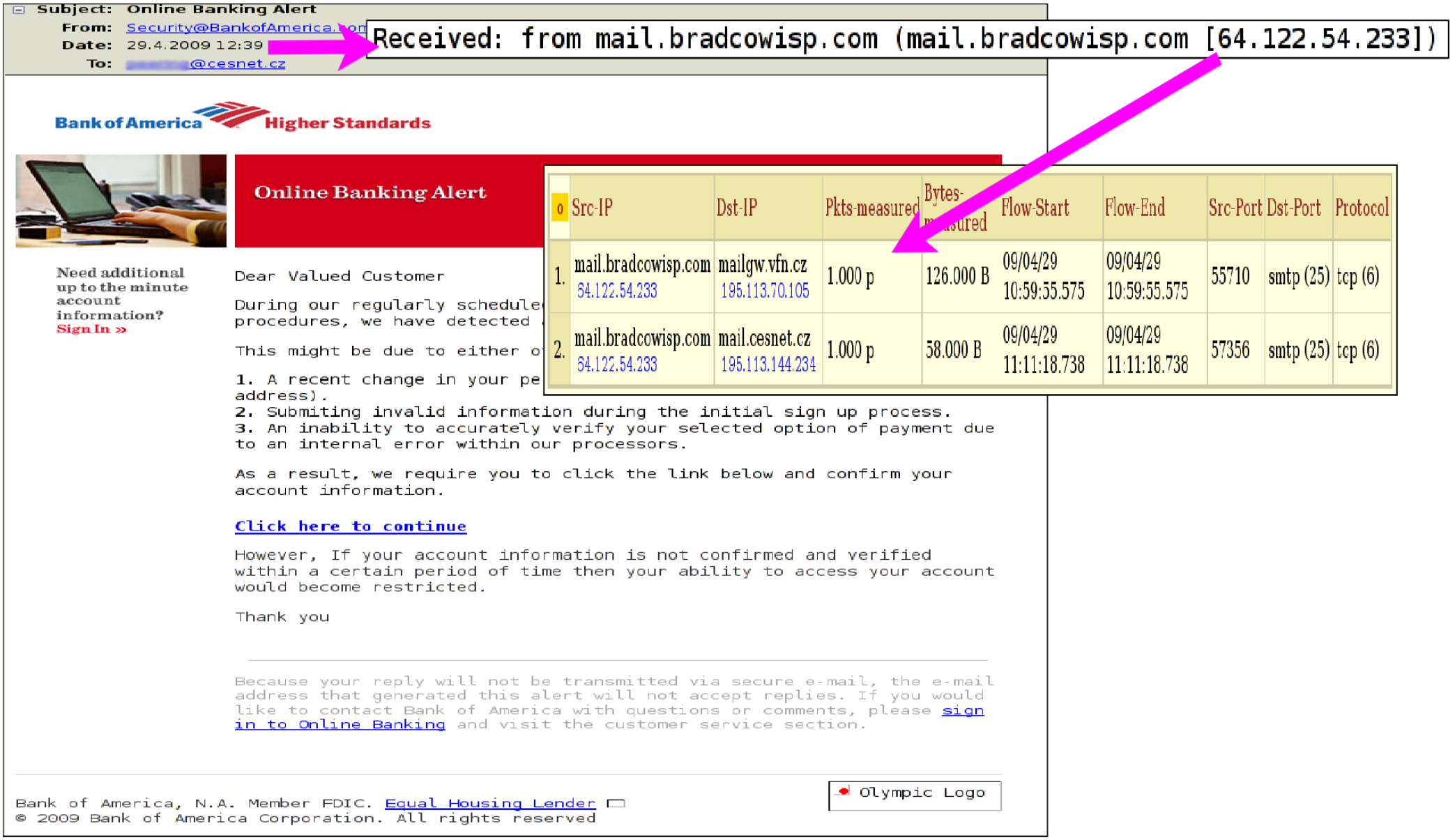
- co je požadováno ?

  B. pokusit se na základě indicií specifikovaných v hlášení nalézt na úrovni provozních informací relevantní informace, včetně plošného rozsahu a vymezení v čase

  - rámcové, neurčité vymezení události
  - zpravidla je třeba nalézt jaká je podstata nebo rozsah problému
    - „chová se to nějak divně“
    - podezření na kompromitované uzly sítě
    - hledání způsobů jakým byl uzel kompromitován
    - hledání rozsahu průniku do sítě

Požadavky plynoucí z bezpečnostních hlášení

- například možný rozsah distribuce phishing mailu z hlediska komunikace na MTA v síti..



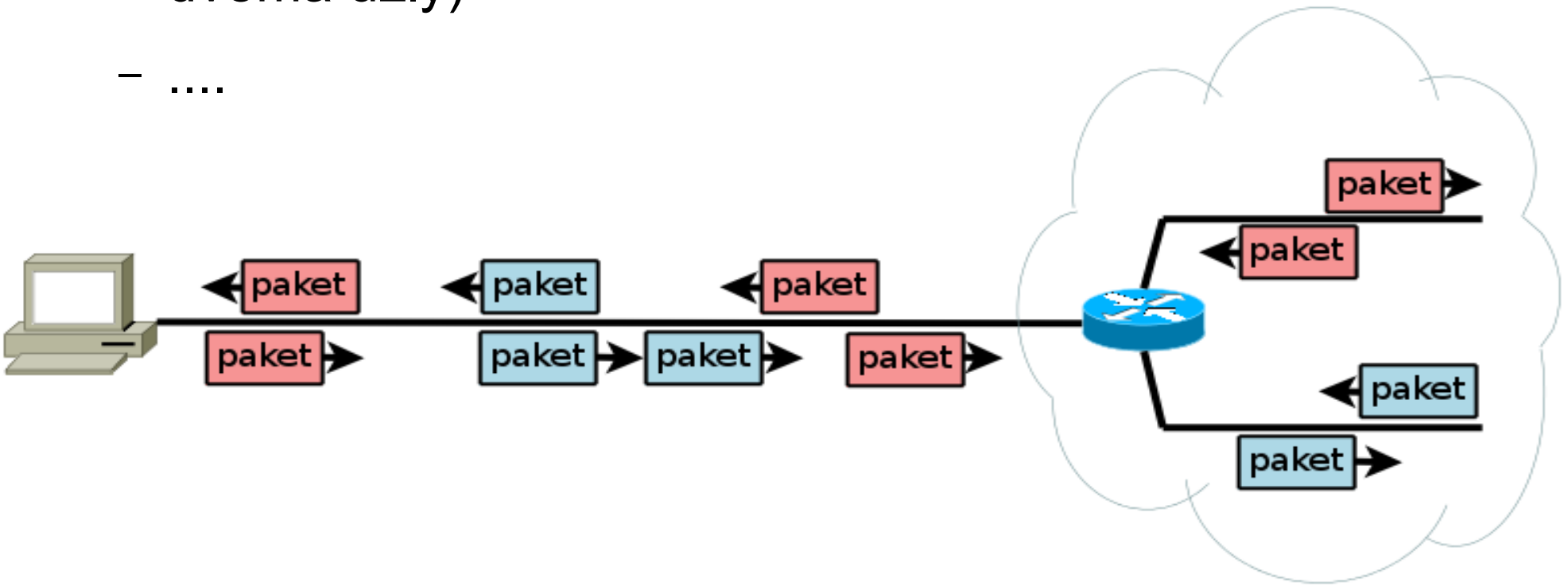
o	Src-IP	Dst-IP	Pkts-measured	Bytes-measured	Flow-Start	Flow-End	Src-Port	Dst-Port	Protocol
1.	mail.bradcowisp.com 64.122.54.233	mailgw.vfn.cz 195.113.70.105	1.000 p	126.000 B	09/04/29 10:59:55.575	09/04/29 10:59:55.575	55710	smtp (25)	tcp (6)
2.	mail.bradcowisp.com 64.122.54.233	mail.cesnet.cz 195.113.144.234	1.000 p	58.000 B	09/04/29 11:11:18.738	09/04/29 11:11:18.738	57356	smtp (25)	tcp (6)

Požadavky plynoucí z bezpečnostních hlášení

- jsou k dispozici informace o IP provozu ?
- jak vznikají ?
- co obsahují ?
- kde se dají získat ?

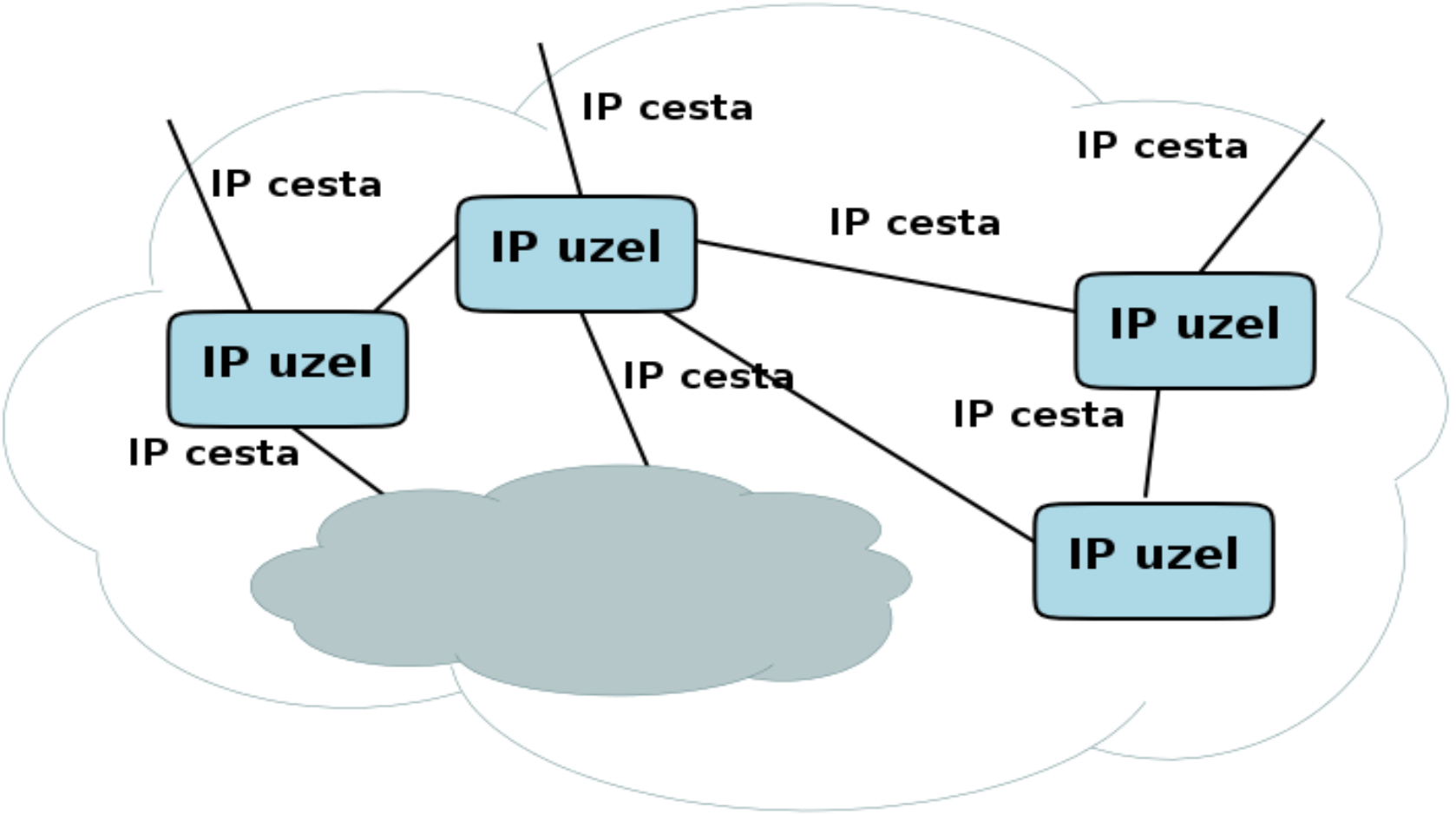
Provozní informace na bázi IP toků

- IP síť (resp. vrstva) – princip přepínání paketů
  - přenášené datové bloky (pakety ~ datagramy) nesou informaci nutnou k přenosu na cílové místo
  - uzel připojený k síti může v principu komunikovat s jakýmkoli jiným připojeným uzlem – zajišťuje funkce sítě (zpravidla existuje více možných cest pro přenos mezi dvěma uzly)
  - ....



Provozní informace na bázi IP toků

- sledování IP provozu – perspektiva pohledu na IP síť



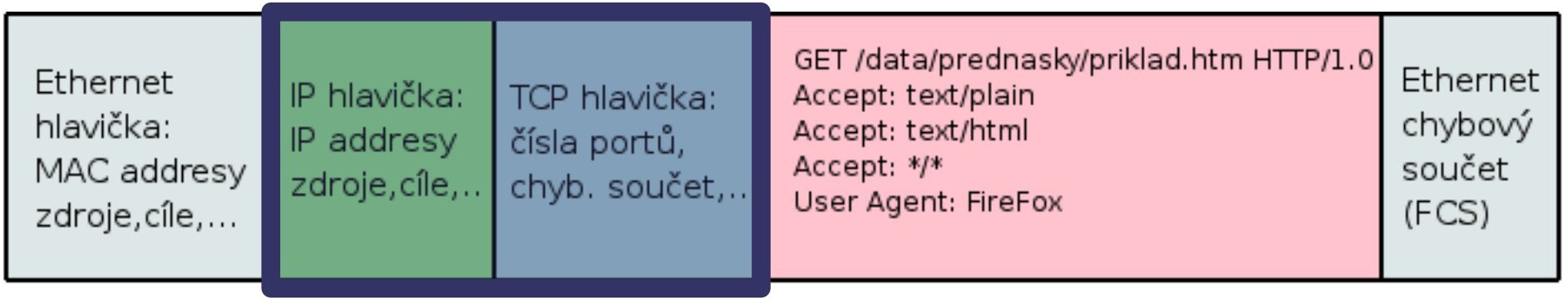
Provozní informace na bázi IP toků

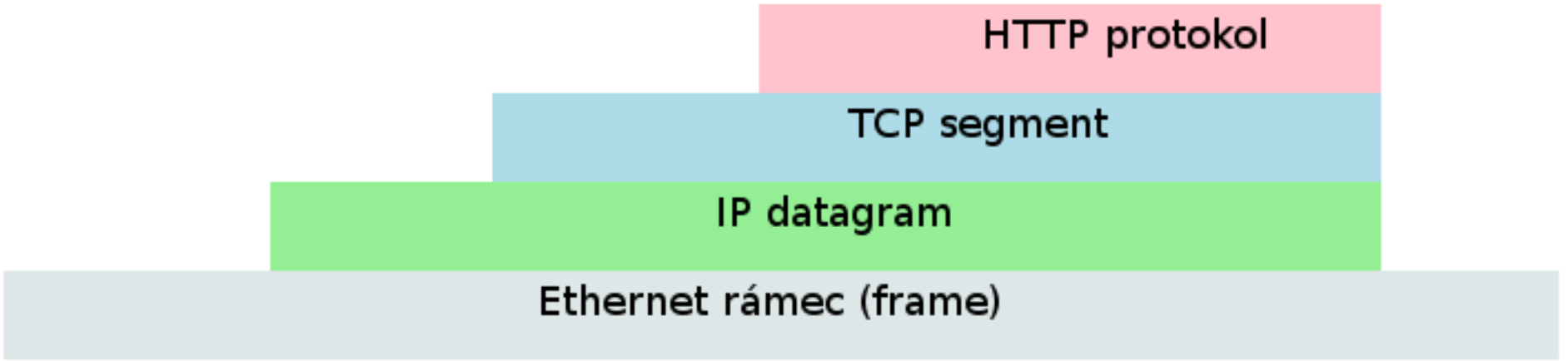
- provozní informace jsou vytvářeny z **údajů získaných z přenášených datových bloků** (datagramů)

  - *původní koncept - NetFlow (Cisco Systems Inc. ™)*

Provozní informace na bázi IP toků

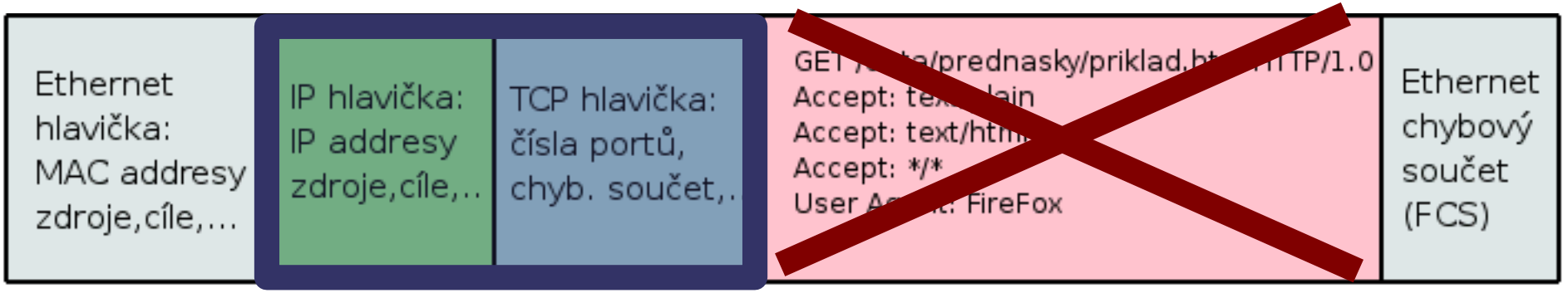
- příklad struktury datového bloku (ethernet rámec), analogie s vrstvami sítě
- **...a datová oblast zdroje provozních informací**





Provozní informace na bázi IP toků

- provozní informace – vztah k ochraně soukromí uživatelů
  - pouze technologické identifikátory
  - žádná vazba na osobní identifikátory
  - žádné informace z oblasti „uživatelských dat“ datového bloku



Provozní informace na bázi IP toků

- provozních informace – základní vlastnosti
  - vybrané informace z hlavičky datagramu TCP/IP
    - tj. informace o **jednosměrném toku**
  - vytvořený záznam dočasně uchován v paměti
    - modifikován s každým datagramem (paketem) příslušným danému toku
  - postupně vzniká **agregovaná informace** o provozu
    - míra agregace je dána časem po který je informace dočasně držena v paměti a množstvím paketů příslušných danému toku přenesených v tomto intervalu

Provozní informace na bázi IP toků

- provozních záznam – struktura

A. identifikátory toku

- základní veličiny identifikující tok
  - IP adresy zdroje, cíle, přenosový protokol, čísla portů (v závislosti na protokolu)
  - *identifikátory rozhraní (zařízení, které data přenášelo a vytvořilo provozní záznam)*
  - *čísla AS zdroje a cíle resp. sousedních (závisí na dostupných informacích)*
  - *příští IP uzel z hlediska přenosu*

– **všechny pakety příslušné danému toku mají tyto údaje stejné - identifikátor toku**

Provozní informace na bázi IP toků

- provozních záznam – struktura

B. objemové ukazatele, časové informace

- celkový objem toku
  - počet bytů, paketů
- rozsah toku v čase
  - čas prvního paketu
  - čas posledního paketu

...v rámci agregačního intervalu

- **agregované údaje, jsou modifikovány s každým dalším paketem příslušným danému toku**

Provozní informace na bázi IP toků

- provozních záznam – struktura

C. atributy toku

- např. Type of Service bity z IP hlavičky
- TCP flags

...logické OR na jednotlivých bitových pozicích přes všechny pakety příslušné danému toku

- **agregované údaje, mohou být modifikovány s každým paketem příslušným danému toku**

Provozní informace na bázi IP toků

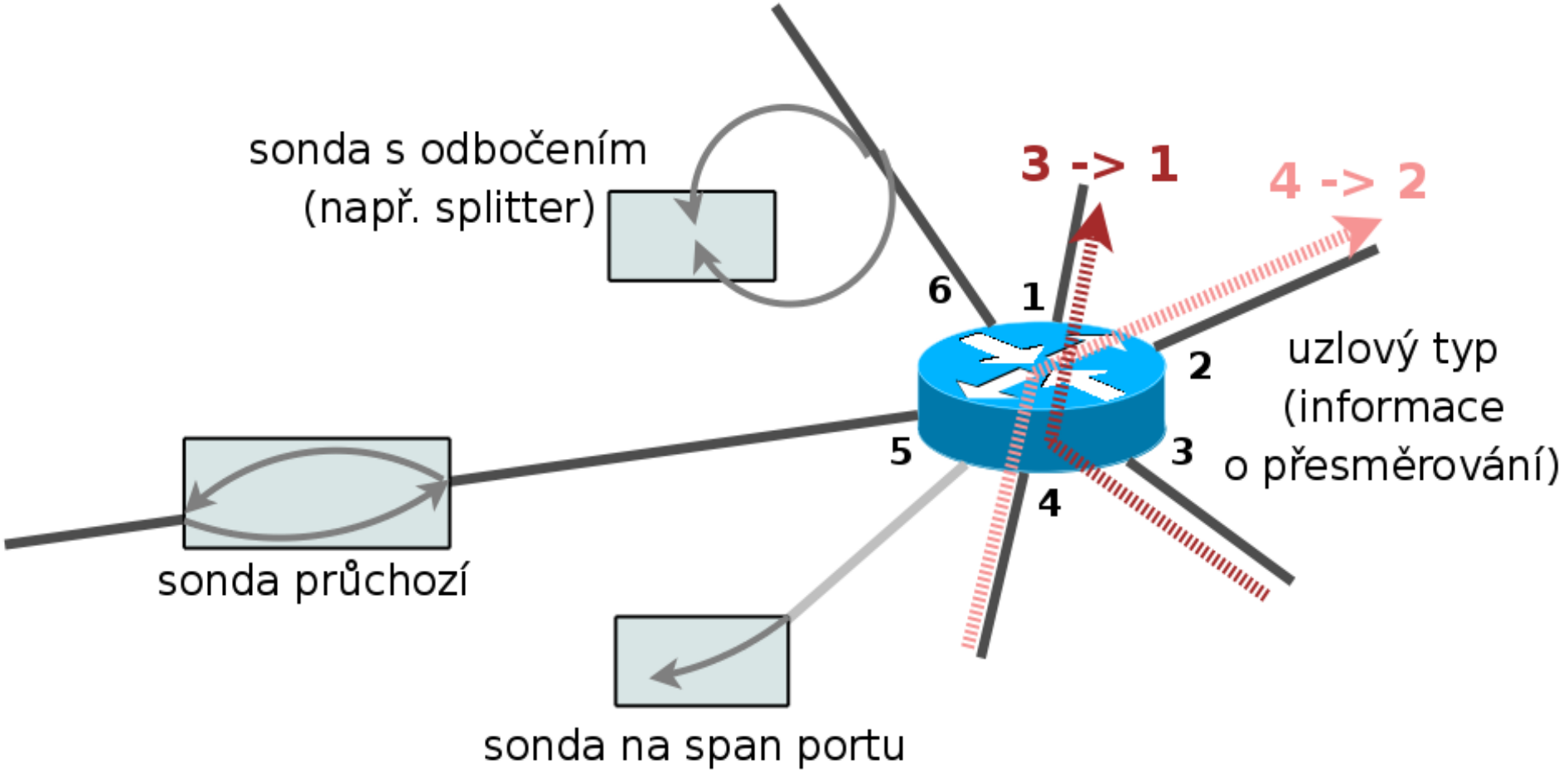
- provozní záznam – „cyklus života“
  - záznam o toku vzniká s prvním paketem toku (v rámci agregačního intervalu)
  - držen v místě vzniku ve vyrovnávací paměti (...a měněn s každým paketem toku...)
  - po expiraci (přirozená nebo nucená) je záznam exportován do míst zpracování (na tzv. kolektory)
    - zpravidla pomocí UDP
    - jedním z několika exportních formátů
      - pevný formát – např. v1, v5, v7 (částečně se liší obsahem, základní struktura stejná)
      - otevřený – v9 (RFC 3954)
        - export informací o struktuře záznamů + export záznamů s identifikátorem odkazujícím na příslušnou strukturu
      - IPFIX (RFCs 3917, 3955, 5101-3)

Zdroje provozních záznamů na bázi IP toků

- technologické členění
  - směrovače (např. Cisco, Juniper)
  - specializované sondy (např. FlowMon - *CESNET z.s.p.o* ™*)*
  - SW řešení (např. tcpflow)

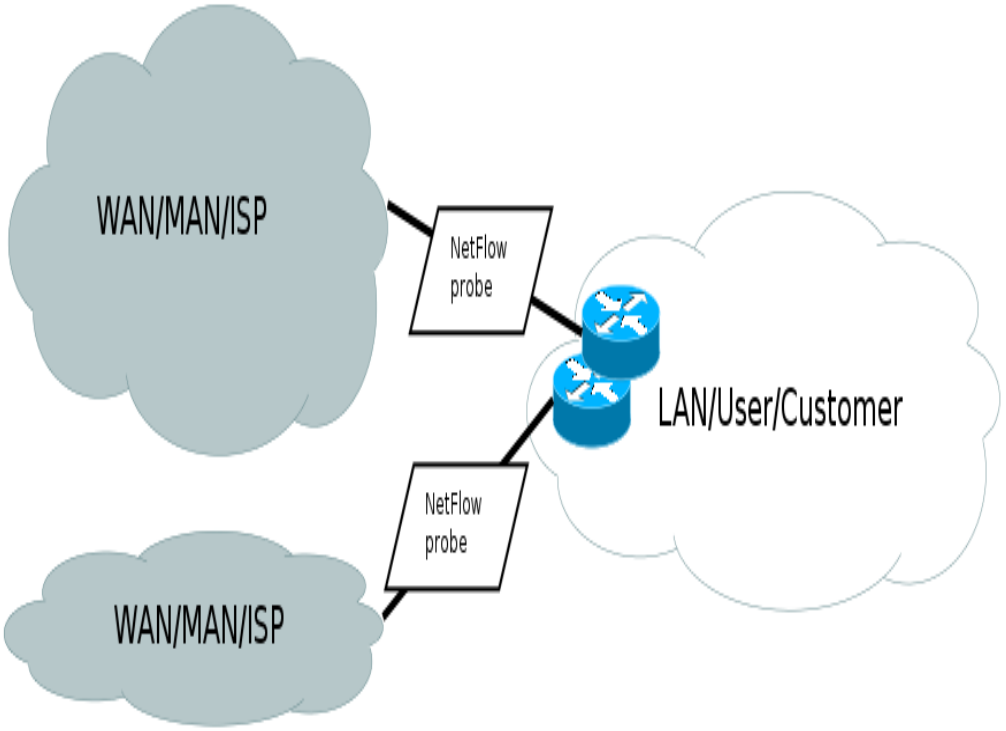
Zdroje provozních záznamů na bázi IP toků

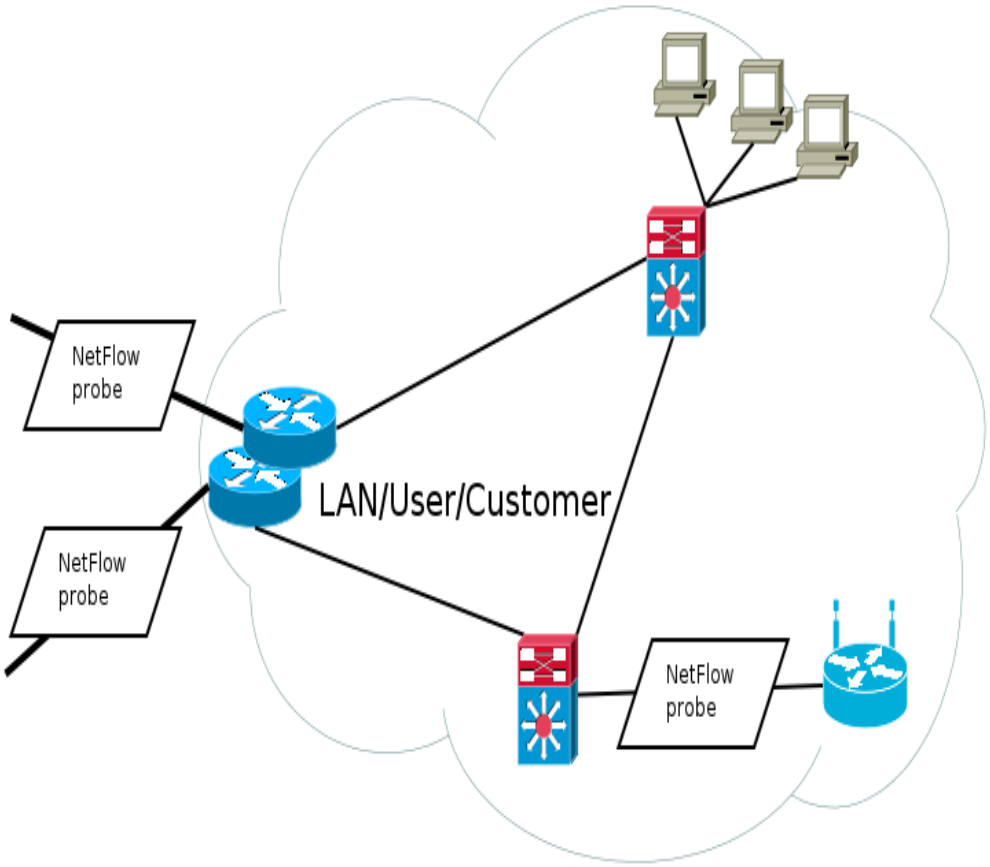
- členění podle charakteru
  - „uzel“
  - „sonda“



Zdroje provozních záznamů na bázi IP toků

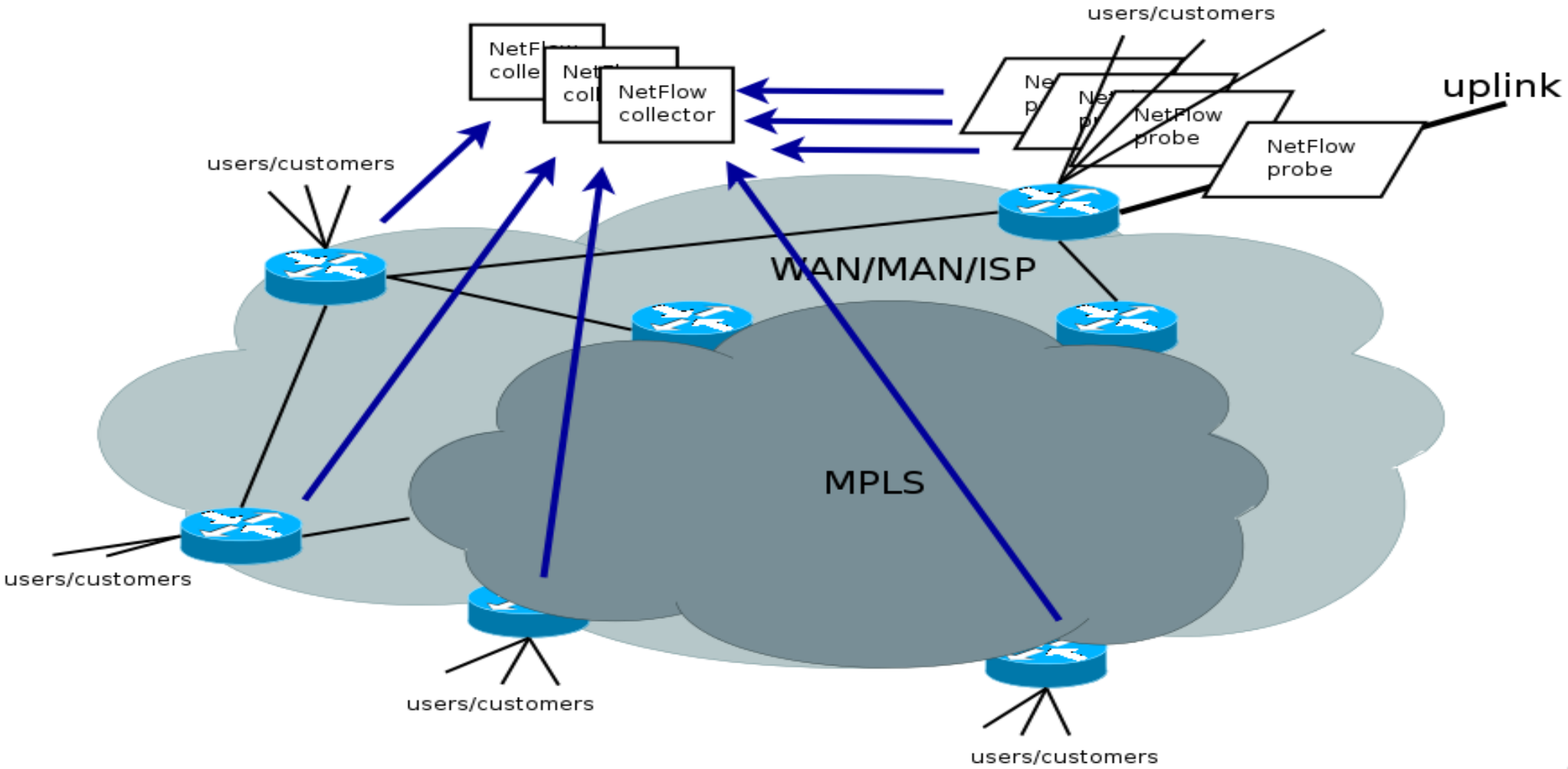
- „rozmístění“ zdrojů provozních záznamů
  - izolované +,- ?





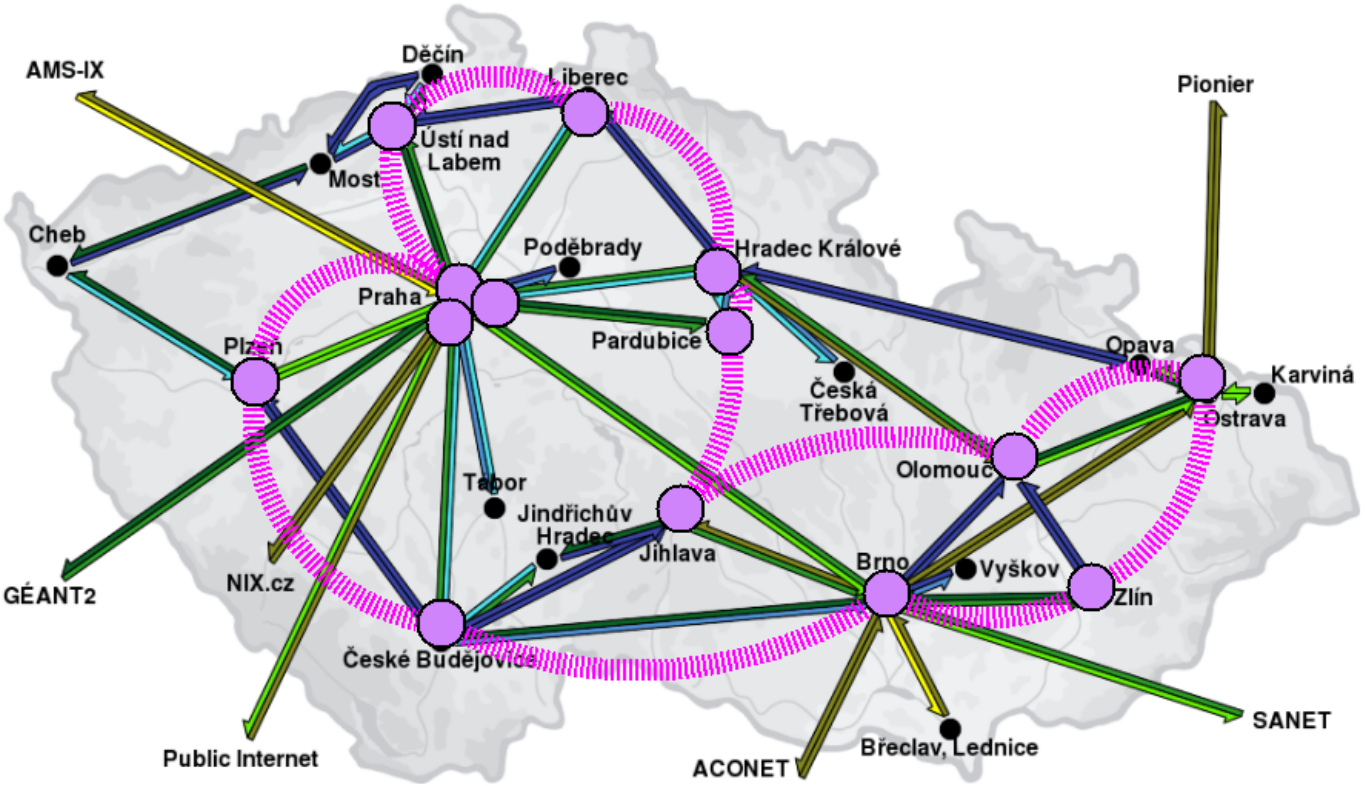
Zdroje provozních záznamů na bázi IP toků

- „rozmístění“ zdrojů provozních záznamů
  - „plošné“ +,- ?



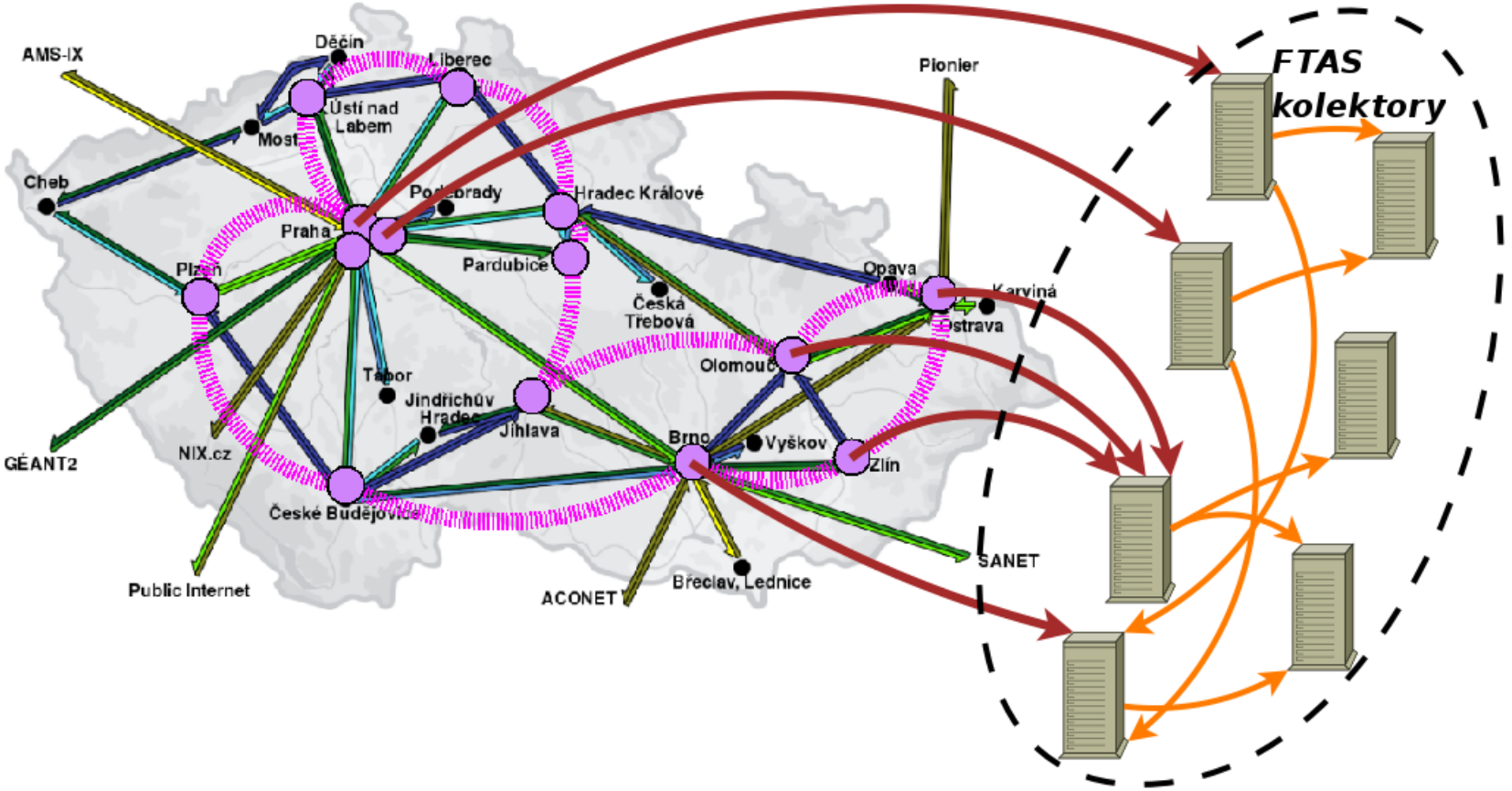
Zdroje provozních záznamů na bázi IP toků

- „rozmístění“ zdrojů provozních záznamů v NREN ČR - síti CESNET2 v rámci plošného souvislého sledování IP provozu
  - obvod pomyslné hranice IP/MPLS páteře
  - směrovače v hraničních PoP
  - většina provozu zpravidla „teče“ přes více zdrojů



Zdroje provozních záznamů na bázi IP toků

- export provozních záznamů v NREN ČR - síti CESNET2 v rámci plošného souvislého sledování IP provozu
  - systém FTAS (vyvíjen sdružením CESNET)
    - distribuované zpracování provozních záznamů na bázi IP toků



Objemy provozních záznamů na bázi IP toků

- množství vytvářených záznamů
  - závislost na objemu provozu
  - **závislost na struktuře provozu**

    A. sledování HD streamu na pracovní stanici uživatele vyústí zpravidla v ~1 Flow záznam (ve směru ke stanici uživatele) za agregační interval, přičemž celkový objem se může pohybovat v desítkách GB (klíčová pole Flow záznamů stejná)

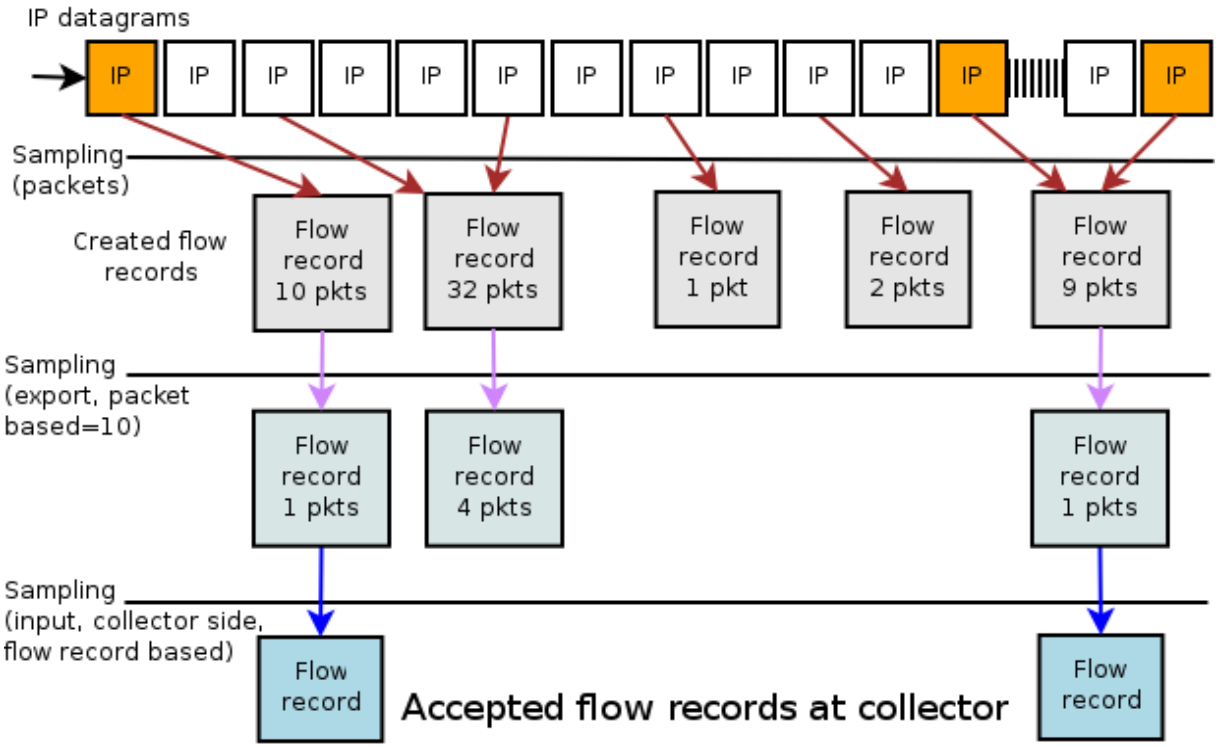
    B. jeden vertikální UDP scan stejné uživatelské stanice vyústí v 65536 Flow záznamů (ve směru ke stanici uživatele), celkový objem zanedbatelný (mění se klíčová pole Flow záznamů)

...efektivně využitelné v oblasti verifikace/detekce většiny typů DoS, DDoS útoků, kdy se zpravidla alespoň jeden z klíčových identifikátorů Flow průběžně mění

Objemy provozních záznamů na bázi IP toků

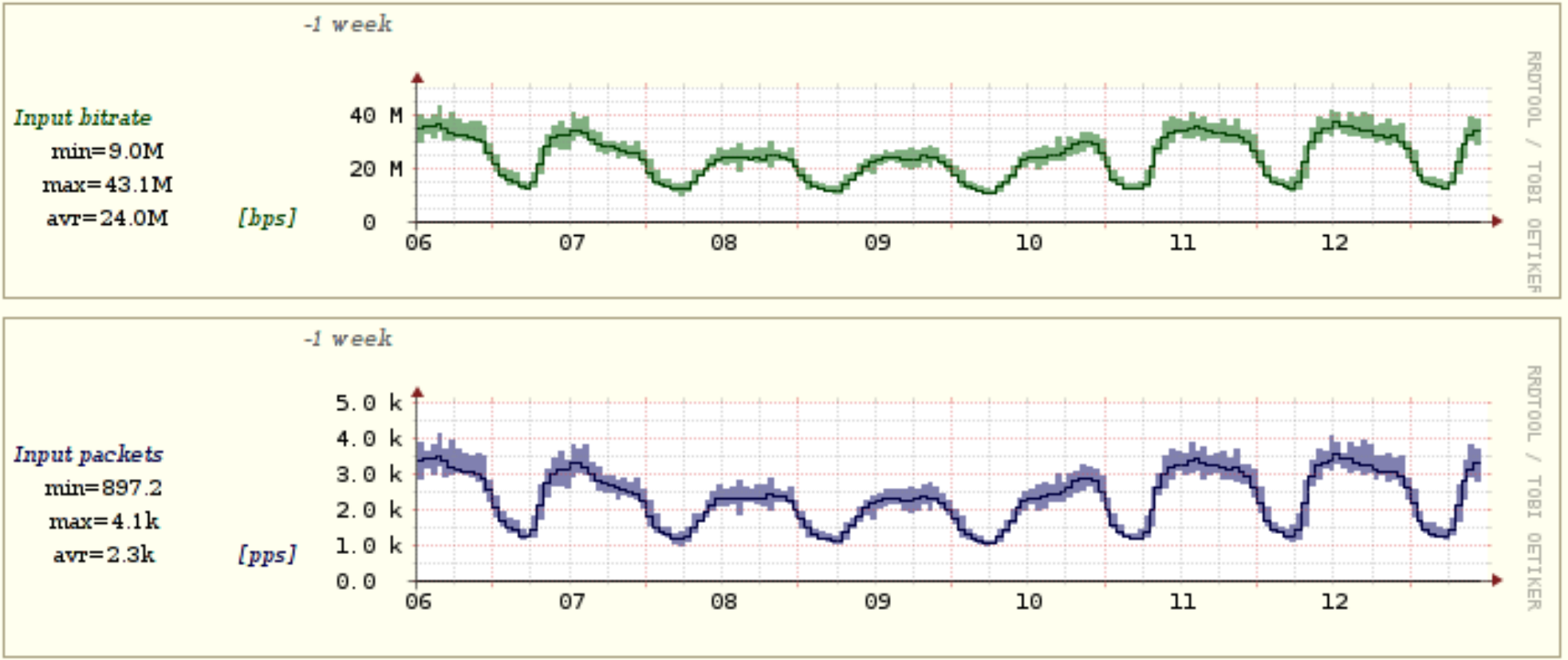
- vzorkování - redukce množství vytvářených/emitovaných záznamů do přijatelných mezí za cenu ztráty vypovídací hodnoty (při plošném sledování částečně kompenzováno)
  - různé modely v závislosti na implementacích, v některých případech povinné
- **nalezení přijatelné míry vzorkování je kritické pro efektivní podporu při řešení bezpečnostních hlášení !!!**

- úroveň paketů na vstupu do Flow stroje
- při exportu z Flow stroje – úroveň paketů (statisticky)
- na vstupu kolektoru – úroveň provozních záznamů



Objemy provozních záznamů na bázi IP toků

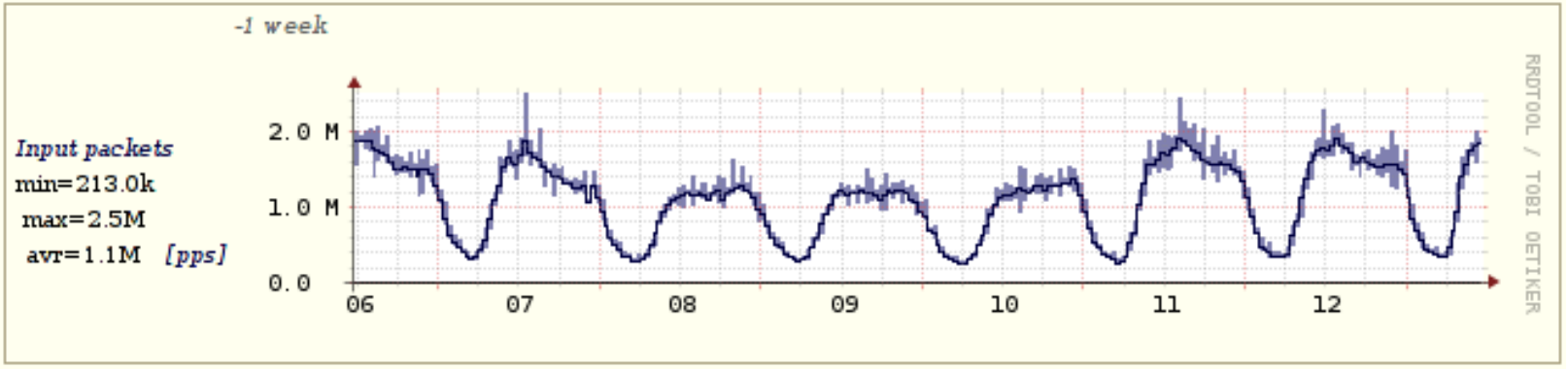
- objem exportovaných provozních záznamů v prostředí sítě CESNET2 – agregovaný objem emitovaný z primárních zdrojů provozních záznamů do systému FTAS



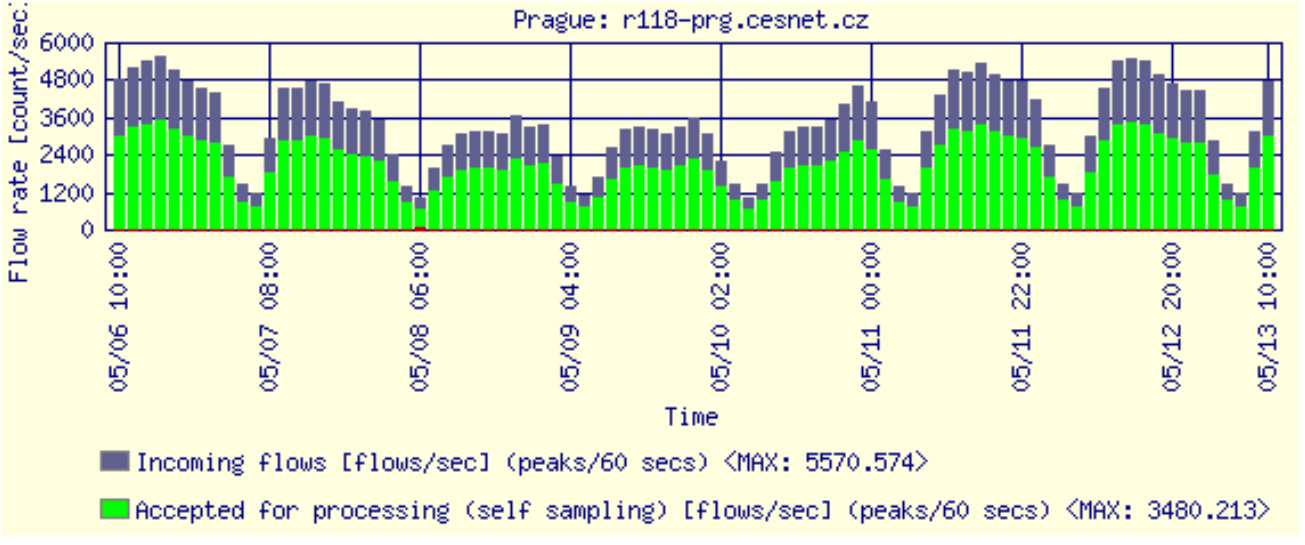
Objemy provozních záznamů na bázi IP toků

- množství generovaných provozních záznamů v prostředí sítě CESNET2 z jednoho zdroje – příklad **A**
  - vzorkování paketů na vstupu směrovače 1:50, vzorkování na vstupu systému pro zpracování 1:1.6

průběh příchozích paketů



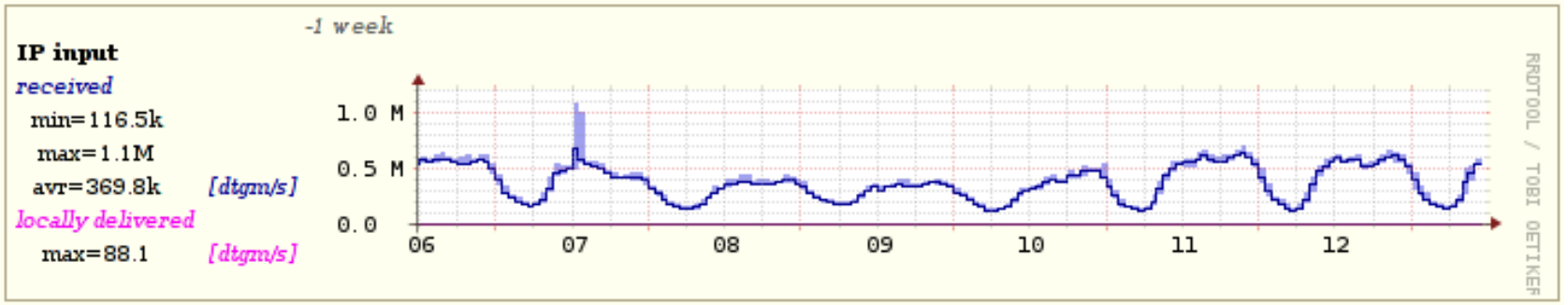
průběh odpovídajících emitovaných provozních záznamů



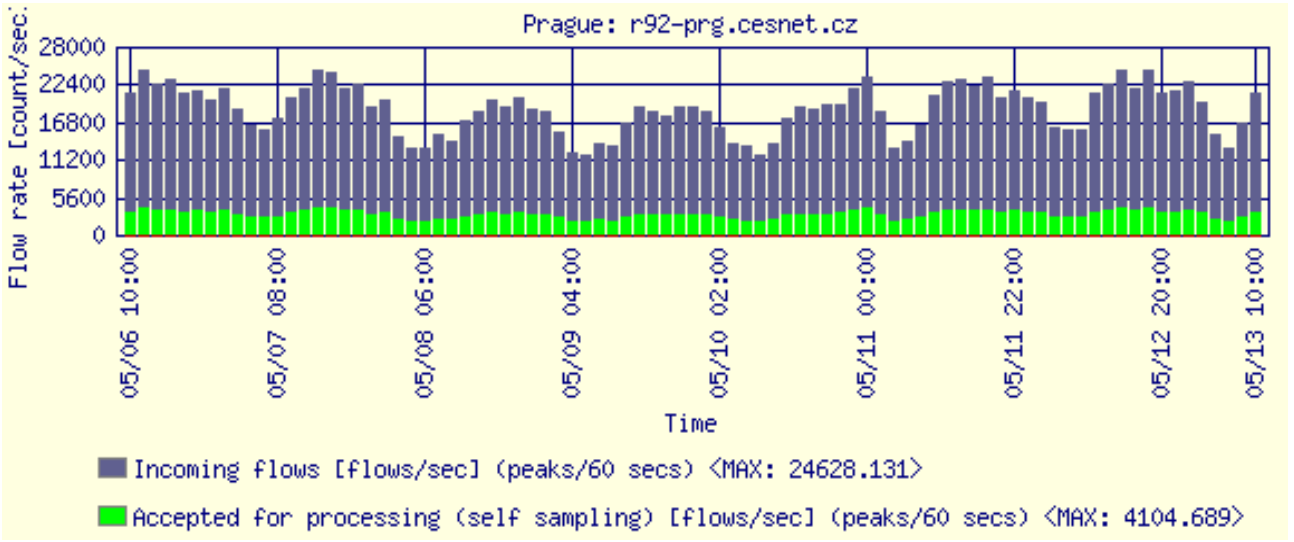
Objemy provozních záznamů na bázi IP toků

- množství generovaných provozních záznamů v prostředí sítě CESNET2 z jednoho zdroje – příklad **B**
  - vzorkování paketů na vstupu směrovače 1:1, vzorkování na vstupu systému pro zpracování 1:6

průběh příchozích IP datagramů

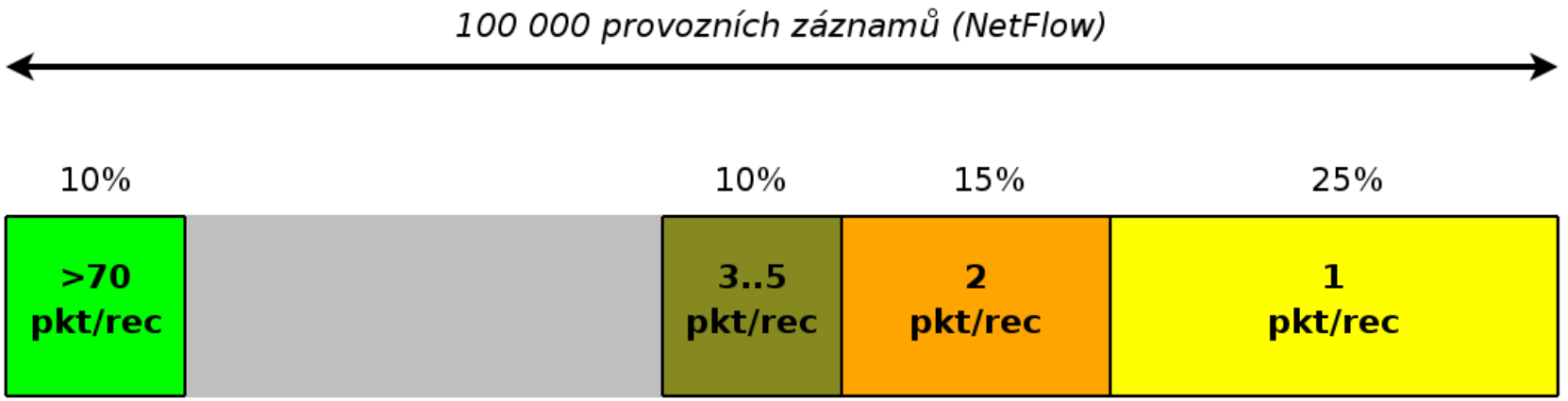


průběh odpovídajících emitovaných provozních záznamů



Objemy provozních záznamů na bázi IP toků

- podstatné aspekty – vždy závislé na konkrétních podmínkách (architektura sítě, politika, způsob využití, ...)
  - míra agregace paketů
    - průměrný počet paketů/1 provozní záznam
    - v síti CESNET2 v průměru cca 70-100 paketů/záznam
  - způsob distribuce paketů
    - rozložení počtu paketů v rámci množiny provozních záznamů
      - velký vliv paketového vzorkování na rozložení

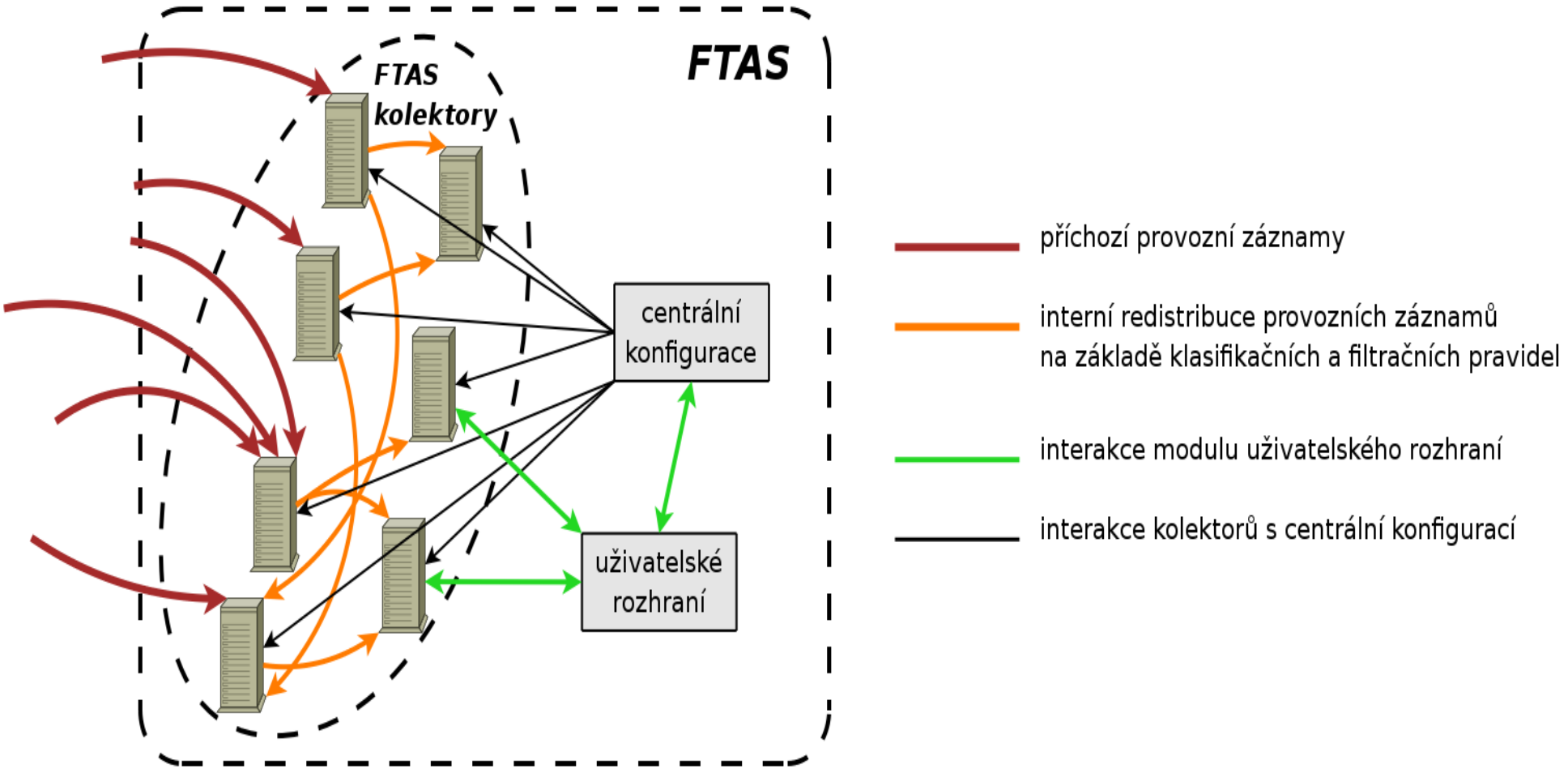


Zpracování provozních záznamů na bázi IP toků

- ...požadavky ve smyslu podpory při řešení bezpečnostních hlášení
  - řešíme děje v minulosti bez jakéhokoli omezení
    - nepřetržité zpracování, ukládání a skladování provozních záznamů po *„nezbytně“* dlouhou dobu s co nejmenší ztrátou vypovídací hodnoty
    - přijatelná doba odezvy při současném vyhledávání
      - komplexní vyhledávací podmínky
      - značný časový rozsah vyhledávání (desítky hodin, jednotky dnů)

Zpracování provozních záznamů na bázi IP toků

- v prostředí sítě CESNET2 – systém FTAS
  - distribuovaný (není podmínkou), škálovatelný do poměru 1 zdroj záznamů na 1 kolektor



Zpracování provozních záznamů na bázi IP toků

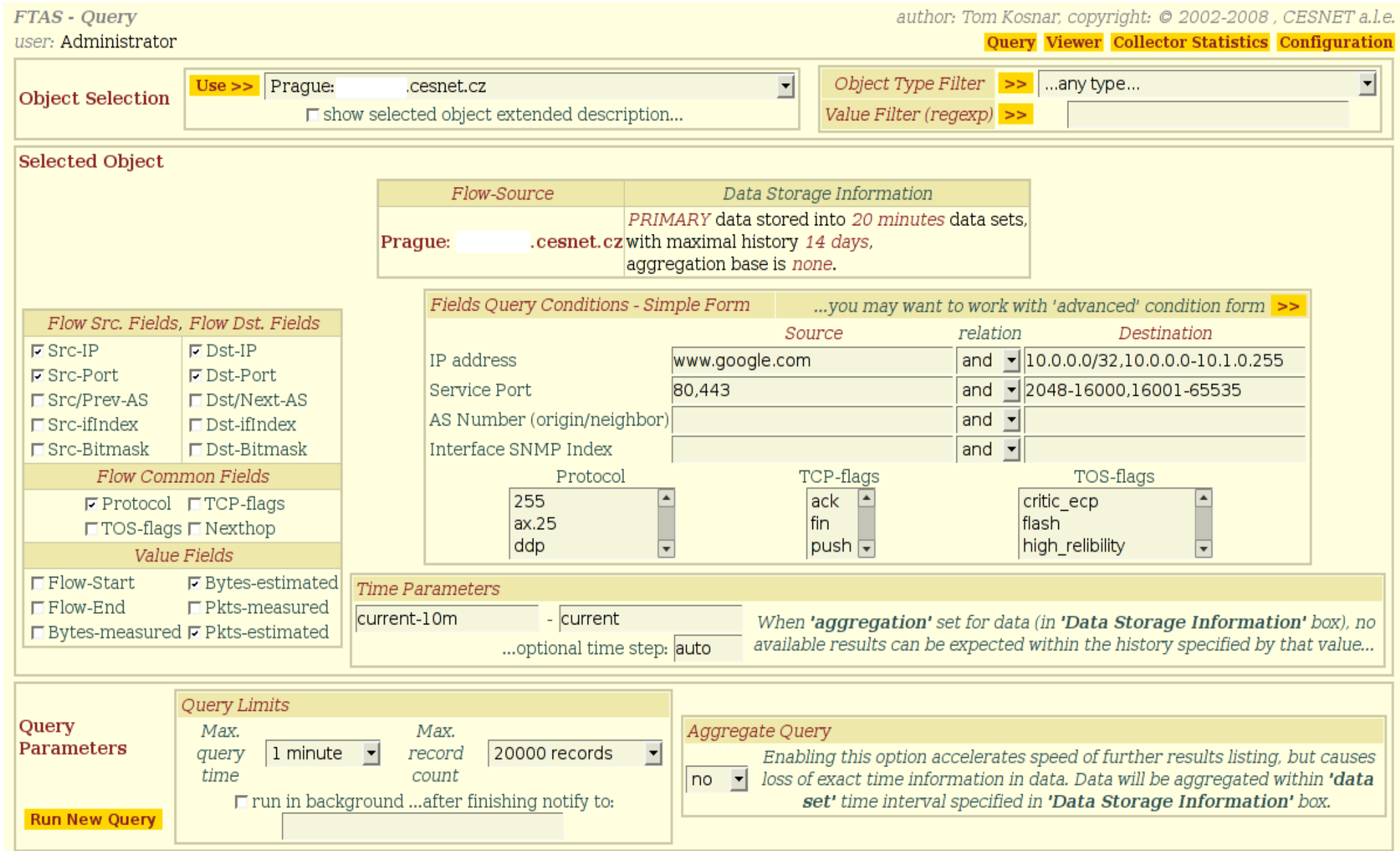
- v prostředí sítě CESNET2 – systém FTAS
  - distribuovatelná úložiště
  - podpora IPv4, IPv6 (jak provozní záznamy, tak interní redistribuce), všechny běžne exportní formáty
  - nastavitelný stabilní poměr „dostupné zdroje/vypovídací hodnota“
    - aktuálně 3000-4000 záznamů/s na kolektor (k uložení)
    - vzorkování na úrovni záznamů 1:1.6-1:7 na vstupu do FTAS a 1:50 na úrovni paketů v případě 1 zdroje
  - libovolně nastavitelné sturuktura i doba uchování záznamů
    - aktuálně uchováváme 1-2 měsíce z primárních zdrojů

Zpracování provozních záznamů na bázi IP toků

- v prostředí sítě CESNET2 – systém FTAS
  - konvenční HW vyšší třídy
    - aktuálně v kategorii Xeon 2.5-3GHz, 2-4G RAM, HW RAID 5 0.5-2TB
  - Debian GNU/Linux, MySQL, Perl, ...
  - všechna UI interaktivní, distribuovaná pomocí WWW
  - koncepce práce s UI - jedno vyhledání, vícenásobná vizualizace
  - statistika využití (posledních 52 týdnů)
    - cca 5000 vyhledání
    - cca 7900 vizualizací

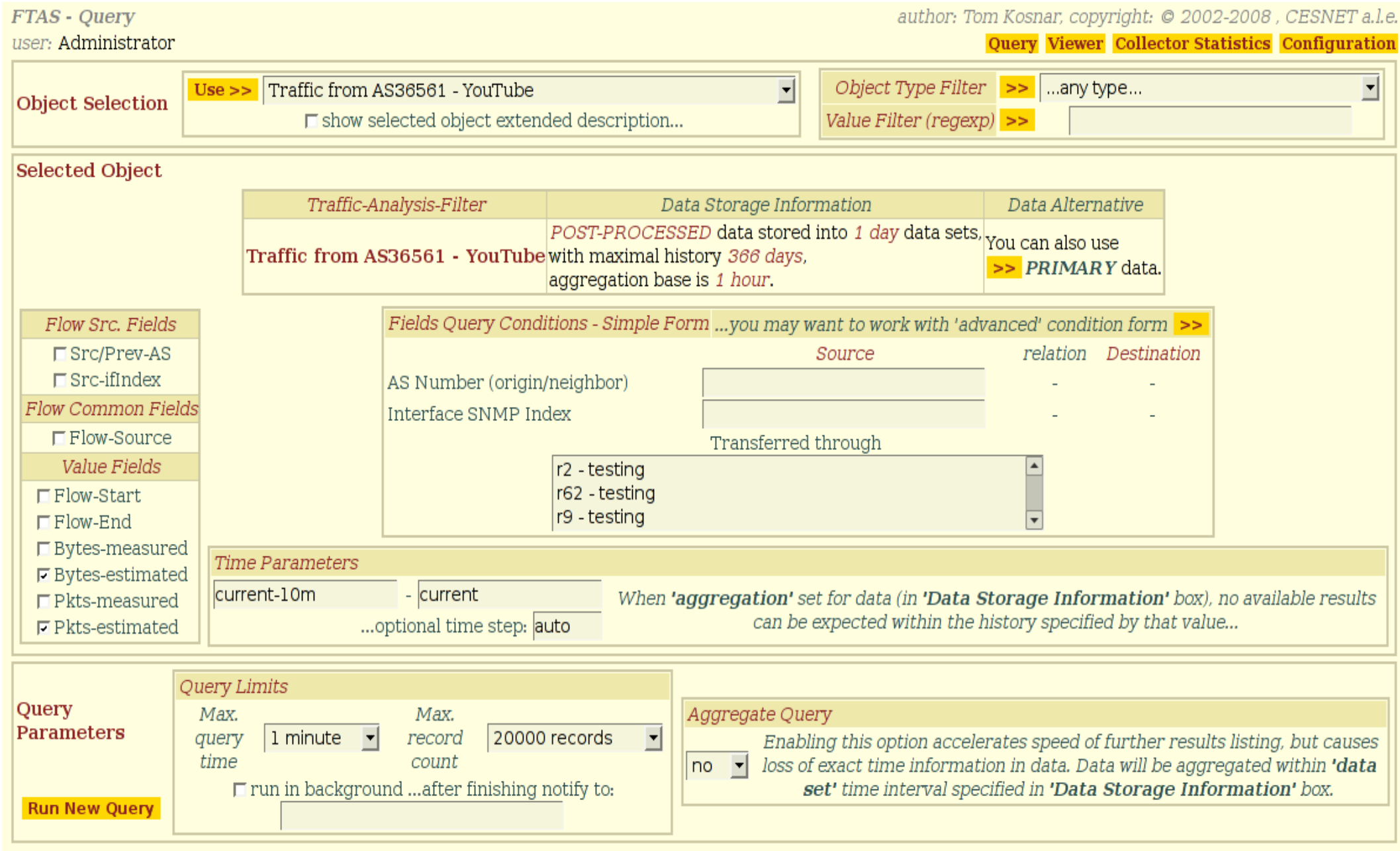
Zpracování provozních záznamů na bázi IP toků

- systém FTAS – jednoduchý formulář pro vyhledávání, ukázka



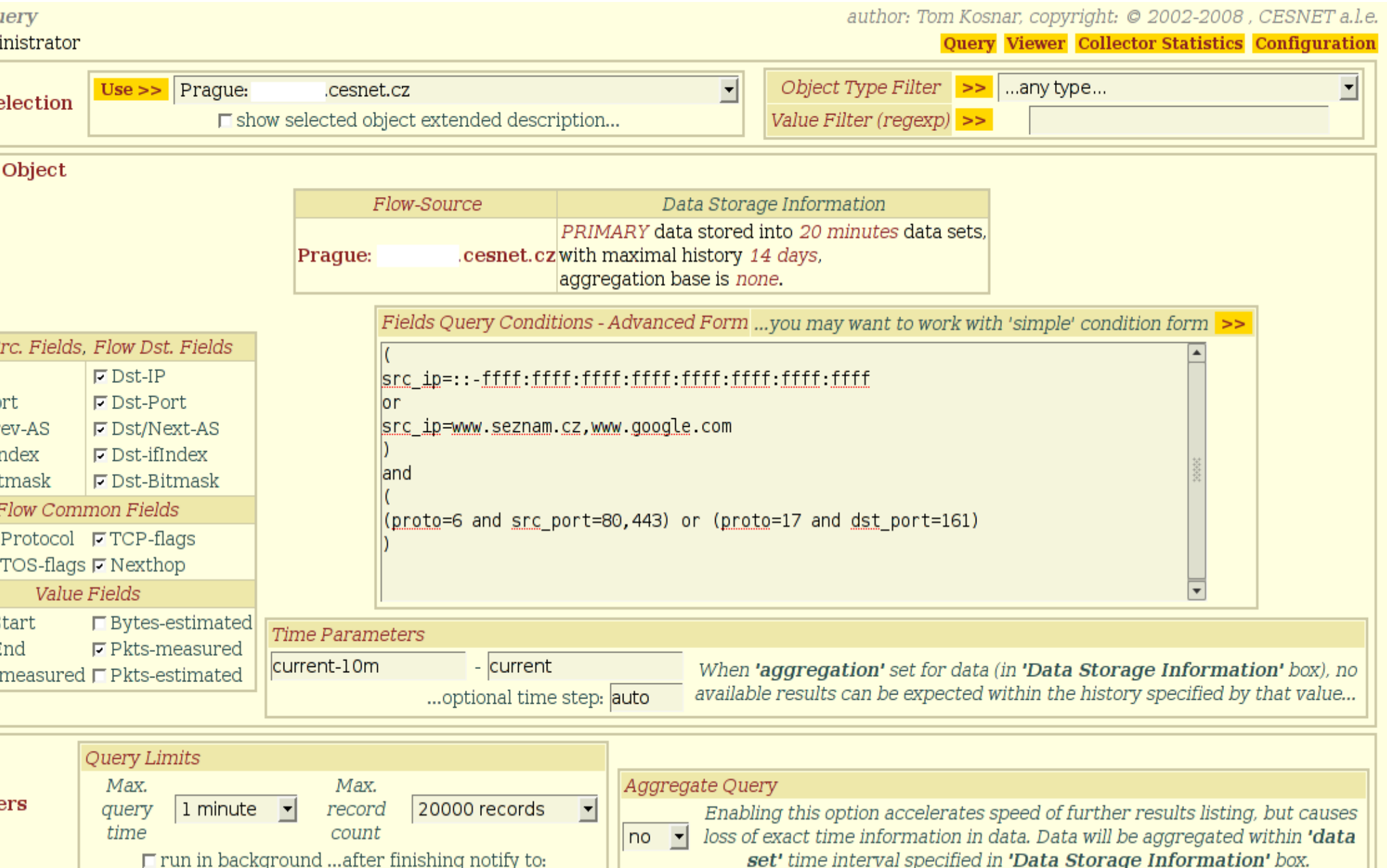
Zpracování provozních záznamů na bázi IP toků

- systém FTAS – jednoduchý formulář pro vyhledávání, ukázka



Zpracování provozních záznamů na bázi IP toků

- systém FTAS – generický formulář pro vyhledávání, ukázka



Zpracování provozních záznamů na bázi IP toků

- systém FTAS – vizualizace, ukázka

FTAS - Viewer — author: Tom Kosnar, copyright: © 2002-20

user: Administrator — Query | Viewer | Collector Sta

Results Selection — Use >> | Prague: .cesnet.cz | 2008/04/24 16:43:19 | << delete this results

show selected results extended description... — save these results permanently as >>

Selected Results

Flow Src. Fields, Flow Dst. Fields		Flow Common Fields	Value Fields	
Src-IP	Src-ifIndex	Protocol	Flow-Start	Pkts-measured
Src-Port	Src-Bitmask	TOS-flags	Flow-End	Pkts-estimated
Src/Prev-AS		TCP-flags	Bytes-measured	Average packet length
Dst-IP	Dst-ifIndex	Nexthop	Bytes-estimated	
Dst-Port	Dst-Bitmask			
Dst/Next-AS				

View Parameters

Display

text/html - ordered by Bytes-estimated in desc. order, aggregation off, recs/page 50

graph - ordered by Bytes-estimated in desc. order, recs/page 15, show summaries/time-step rather than rates

resolve host names | hide viewer form | hide links in results | send (*.tar) with directory name FTAS

Results

o	>	Src-IP	Dst-IP	Nexthop	Src-ifIndex	Dst-ifIndex	Pkts-measured	Bytes-measured	Flow-Start	Flow-End	Src-Port	Dst-Port	TCP-flags	Protocol	TOS-flags	Src/Pr
1.		2001:1528:124:100::225:69	2001:718:1c01:165:f0ef:5090:f06c:2f59		3	0	0.439 kp	0.587 MB	08/04/24 16:33:06.797	08/04/24 16:35:33.613	www (80)	49820		tcp (6)	routine(0)	
2.		66.249.91.99	1 115.250	195.11 6.157	69	1	0.320 kp	0.346 MB	08/04/24 16:38:15.666	08/04/24 16:38:44.018	https (443)	60092		tcp (6)	routine(0)	AS151
3.		66.249.91.99	1 2.249.124	195.11 6.157	69	1	0.327 kp	0.322 MB	08/04/24 16:36:05.519	08/04/24 16:36:53.327	www (80)	2499		tcp (6)	routine(0)	AS151
4.		66.249.91.99	1 2.249.124	195.11 6.157	69	1	0.337 kp	0.311 MB	08/04/24 16:39:31.842	08/04/24 16:40:22.850	www (80)	2557		tcp (6)	routine(0)	AS151
5.		2001:6b0:e:2018::158	2001:718:1801:1a02:200:5efe:93e4:104c		4	0	0.250 kp	0.301 MB	08/04/24 16:39:09.293	08/04/24 16:39:14.349	www (80)	51840		tcp (6)	routine(0)	
6.		2001:640:20:ff00::194	2001:718:1c01:163:255e:e692:6d4f:23bf		69	0	0.213 kp	0.299 MB	08/04/24 16:42:44.193	08/04/24 16:42:52.257	www (80)	1403		tcp (6)	immediate(2)	
7.		66.249.91.104	1 .207.165	195.11 6.157	69	1	0.234 kp	0.271 MB	08/04/24 16:38:08.359	08/04/24 16:38:10.343	https (443)	2617		tcp (6)	routine(0)	AS151
8.		66.249.91.99	1 6.152.233	195.11 6.157	69	1	0.211 kp	0.223 MB	08/04/24	08/04/24	www (80)	2299		tcp (6)	routine(0)	AS151

Zpracování provozních záznamů na bázi IP toků

- systém FTAS – vizualizace s agregací, ukázka

FTAS - Viewer *author: Tom Kosnar, copyright:*

user: Administrator Query Viewer C

Results Selection Use >> Prague: .cesnet.cz 2008/04/24 16:43:19

show selected results extended description... *save these results permanently as* >>

Selected Results

Flow Src. Fields, Flow Dst. Fields	*Flow Common Fields*	*Value Fields*
Src-IP, Src-ifIndex, Src-Port, Src-Bitmask, Src/Prev-AS	Protocol, TOS-flags, TCP-flags, Nexthop	Flow-Start, Pkts-measured, Flow-End, Pkts-estimated, Bytes-measured, Average packet length, Bytes-estimated
Dst-IP, Dst-ifIndex, Dst-Port, Dst-Bitmask, Dst/Next-AS		

View Parameters

Display

text/html - ordered by Bytes-estimated in desc. order, aggregation on , recs/page 50

graph - ordered by Bytes-estimated in desc. order, recs/page 15 , show summaries/time-step rather than rates

resolve host names hide viewer form hide links in results send (*.tar) with directory name FTAS

Results

o	Src-IP	Pkts-measured	Bytes-measured	Flow-Start	Flow-End	Src-Port	Protocol	Src/Prev-AS
1.	66.249.91.99	6.542 kp	4.841 MB	08/04/24 16:32:51.681	08/04/24 16:43:24.898	www (80)	tcp (6)	AS15169
2.	66.249.91.103	4.597 kp	3.339 MB	08/04/24 16:33:11.572	08/04/24 16:43:24.324	www (80)	tcp (6)	AS15169
3.	66.249.91.104	4.167 kp	2.804 MB	08/04/24 16:32:59.973	08/04/24 16:43:21.154	www (80)	tcp (6)	AS15169
4.	66.249.91.147	3.798 kp	2.471 MB	08/04/24 16:32:56.453	08/04/24 16:43:24.455	www (80)	tcp (6)	AS15169
5.	77.75.76.3	2.336 kp	1.938 MB	08/04/24 16:33:22.917	08/04/24 16:43:23.750	www (80)	tcp (6)	AS5610
6.	66.249.91.99	0.922 kp	0.684 MB	08/04/24 16:33:22.584	08/04/24 16:42:52.559	https (443)	tcp (6)	AS15169
7.	2001:1528:124:100::225:69	0.439 kp	0.587 MB	08/04/24 16:33:06.797	08/04/24 16:35:33.613	www (80)	tcp (6)	
8.	66.249.91.104	0.449 kp	0.398 MB	08/04/24 16:33:22.823	08/04/24 16:42:24.899	https (443)	tcp (6)	AS15169
9.	2001:6b0:e:2018::158	0.251 kp	0.301 MB	08/04/24 16:39:09.293	08/04/24 16:39:26.534	www (80)	tcp (6)	
10.	2001:640:20:ff00::194	0.213 kp	0.299 MB	08/04/24 16:42:44.193	08/04/24 16:42:52.257	www (80)	tcp (6)	

Zpracování provozních záznamů na bázi IP toků

- systém FTAS – grafická vizualizace, ukázka

FTAS - Viewer *author: Tom Kosnar, copy*
user: Administrator Query Vie

Results Selection Use >> Prague: .cesnet.cz 2008/04/24 16:43:19
show selected results extended description... *save these results permanently as* >>

Selected Results

Flow Src. Fields, Flow Dst. Fields		*Flow Common Fields*	*Value Fields*	
Src-IP	Src-ifIndex	Protocol	Flow-Start	Pkts-measured
Src-Port	Src-Bitmask	TOS-flags	Flow-End	Pkts-estimated
Src/Prev-AS		TCP-flags	Bytes-measured	Average packet length
Dst-IP	Dst-ifIndex	Nexthop	Bytes-estimated	
Dst-Port	Dst-Bitmask			
Dst/Next-AS				

View Parameters

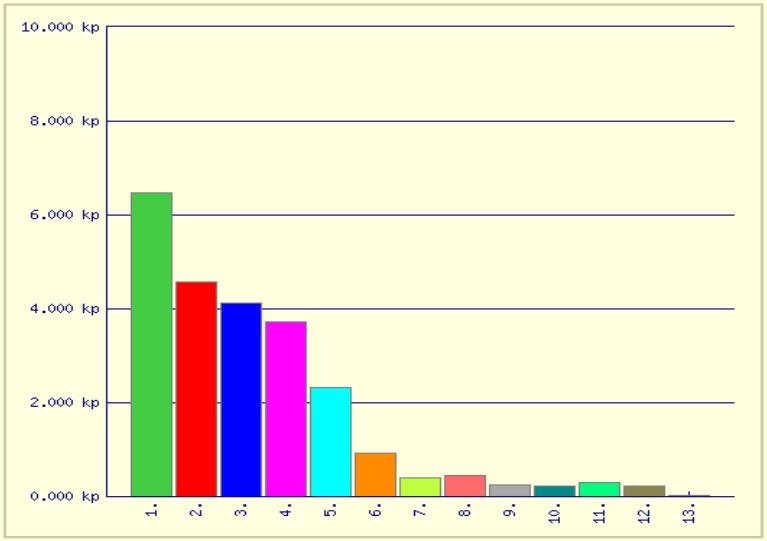
Display

text/html - ordered by Bytes-estimated in desc. order, aggregation on , recs/page 50
graph - ordered by Bytes-estimated in desc. order, recs/page 15 , show summaries/time-step rather than ra

resolve host names hide viewer form hide links in results send (*.tar) with directory name FTAS

Pkts-measured: *summary per time range*

Summary			
	In graph	23.976 kp	100.00%
	Rest of results	0.000 kp	0.00%
	Total	23.976 kp	100.00%

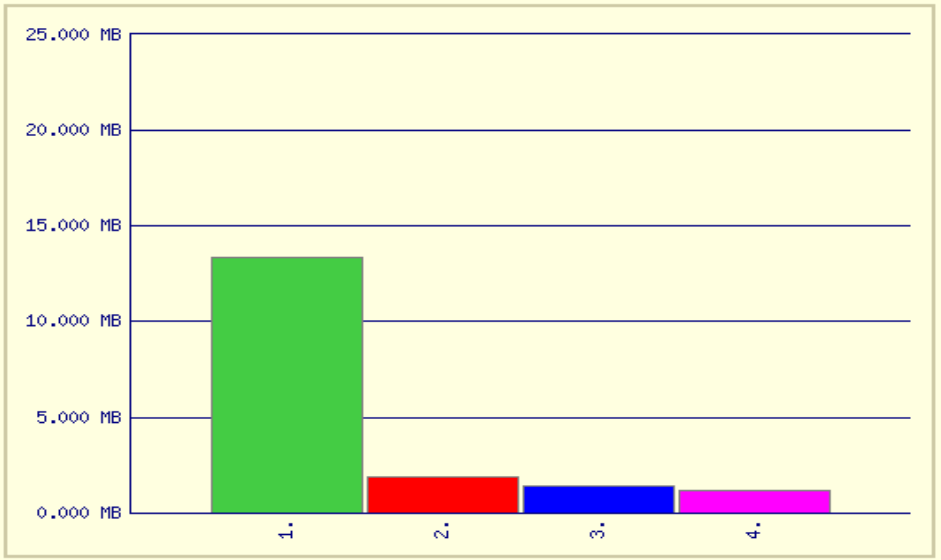


	Src-IP	Src-Port	Protocol	Src/Prev-AS	Pkts-measured
1. >	ik-in-f99.google.com 66.249.91.99	www (80)	tcp (6)	AS15169	6.478 kp
2. >	ik-in-f103.google.com 66.249.91.103	www (80)	tcp (6)	AS15169	4.568 kp
3. >	ik-in-f104.google.com 66.249.91.104	www (80)	tcp (6)	AS15169	4.114 kp
4. >	ik-in-f147.google.com 66.249.91.147	www (80)	tcp (6)	AS15169	3.718 kp
5. >	www.seznam.cz 77.75.76.3	www (80)	tcp (6)	AS5610	2.331 kp
6. >	ik-in-f99.google.com 66.249.91.99	https (443)	tcp (6)	AS15169	0.922 kp
7. >	2001:1528:124:100::225:69	www (80)	tcp (6)		0.403 kp
8. >	ik-in-f104.google.com 66.249.91.104	https (443)	tcp (6)	AS15169	0.449 kp
9. >	2001:6b0:e:2018::158	www (80)	tcp (6)		0.251 kp
10. >	2001:640:20:ff00::194	www (80)	tcp (6)		0.213 kp
11. >	ik-in-f147.google.com 66.249.91.147	https (443)	tcp (6)	AS15169	0.292 kp
12. >	ik-in-f103.google.com 66.249.91.103	https (443)	tcp (6)	AS15169	0.224 kp
13. >	2001:1488:d91f:cd70::cd72	www (80)	tcp (6)		14.000 p

Zpracování provozních záznamů na bázi IP toků

- systém FTAS – grafická vizualizace, ukázka

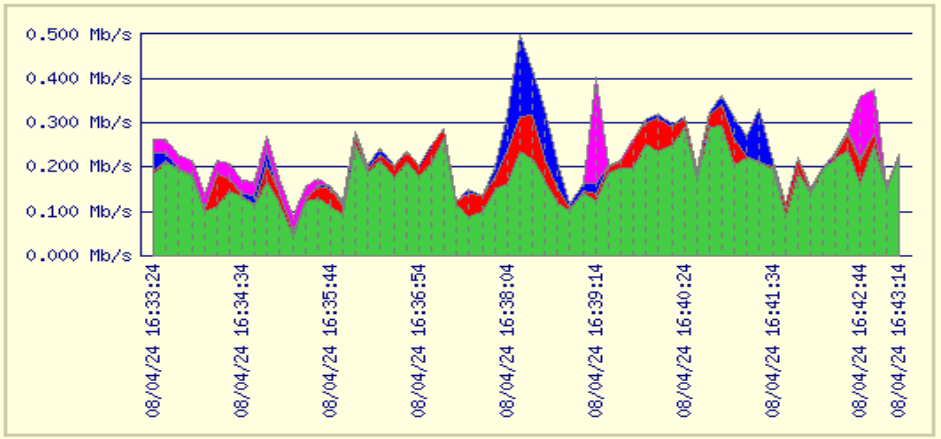
Bytes-measured: *summary per time range*



Summary			
	In graph	17.812 MB	100.00%
	Rest of results	0.000 MB	0.00%
	Total	17.812 MB	100.00%

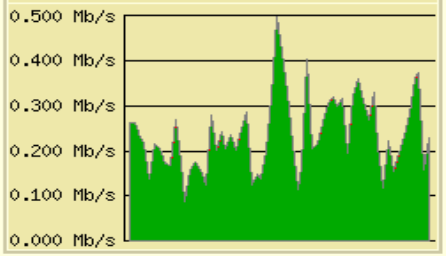
		Src-Port	Protocol	Src/Prev-AS	Bytes-measured
1.	>	www (80)	tcp (6)	AS15169	13.321 MB
2.	>	www (80)	tcp (6)	AS5610	1.935 MB
3.	>	https (443)	tcp (6)	AS15169	1.406 MB
4.	>	www (80)	tcp (6)		1.150 MB

Bytes-measured: *rates*



Summary			
	In graph	17.812 MB	100.00%
	Rest of results	0.000 MB	0.00%
	Total	17.812 MB	100.00%

Summary in Time

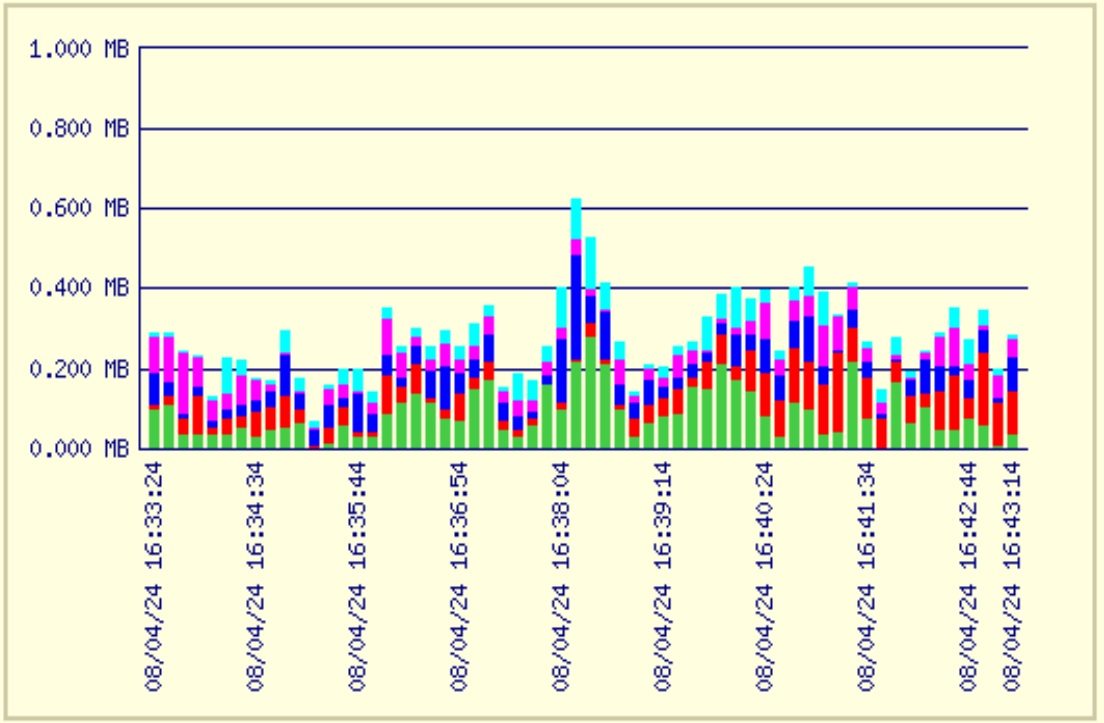


		Src-Port	Protocol	Src/Prev-AS	Bytes-measured
1.	>	www (80)	tcp (6)	AS15169	13.321 MB
2.	>	www (80)	tcp (6)	AS5610	1.935 MB
3.	>	https (443)	tcp (6)	AS15169	1.406 MB
4.	>	www (80)	tcp (6)		1.150 MB

Zpracování provozních záznamů na bázi IP toků

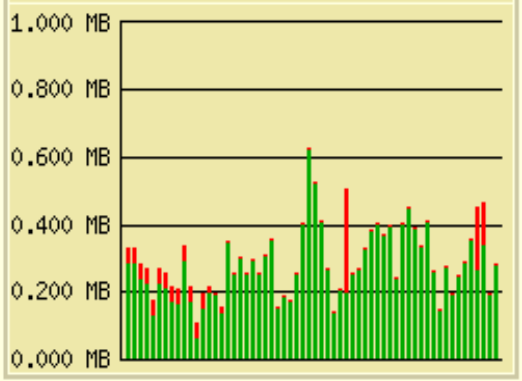
- systém FTAS – grafická vizualizace, ukázka

Bytes-measured: *summaries per time steps*



Summary			
	In graph	16.662 MB	93.54%
	Rest of results	1.150 MB	6.46%
	Total	17.812 MB	100.00%

Summary in Time



o >	Src-IP	Bytes-measured
1. >	ik-in-f99.google.com 66.249.91.99	5.481 MB
2. >	ik-in-f103.google.com 66.249.91.103	3.481 MB
3. >	ik-in-f104.google.com 66.249.91.104	3.176 MB
4. >	ik-in-f147.google.com 66.249.91.147	2.589 MB
5. >	www.seznam.cz 77.75.76.3	1.935 MB

Zhodnocení

- +informace o tom, jak jsou v síti nebo v jejích částech data skutečně přenášena
- +výrazně zvyšuje efektivitu řešení provozních anomálií a incidentů
- +mnoho vedlejších efektů souvisejících nejen s bezpečnostní oblastí (optimalizace směrování, využití zdrojů apod.)
- -vypovídací hodnota úměrná požadavkům na zdroje (objem dat ke zpracování, doba uchování...)
- -řešení na míru konkrétním požadavkům v konkrétních podmínkách dané sítě (nároky na flexibilita nástrojů, gramotnost personálu, atd...)
- není samospasitelné – je dalším článkem celé soustavy metod a nástrojů pro řešení bezpečnostních hlášení, ale velmi hodnotným...

???