NetFlow és NFSen
Flow analízis a HBONE-ban

Mohácsi János, NIIF <mohacsi@niif.hu>
Kiss Gábor, NIIF <kissg@niif.hu>

2006.11.10.

Áttekintés

- Bevezetés
- Netflow v?– áttekintés
- Netflow Cisco környezetben
- Netflow kollektorok
- NFSen
  - Áttekintés
  - Anomália detekció

Motivációk

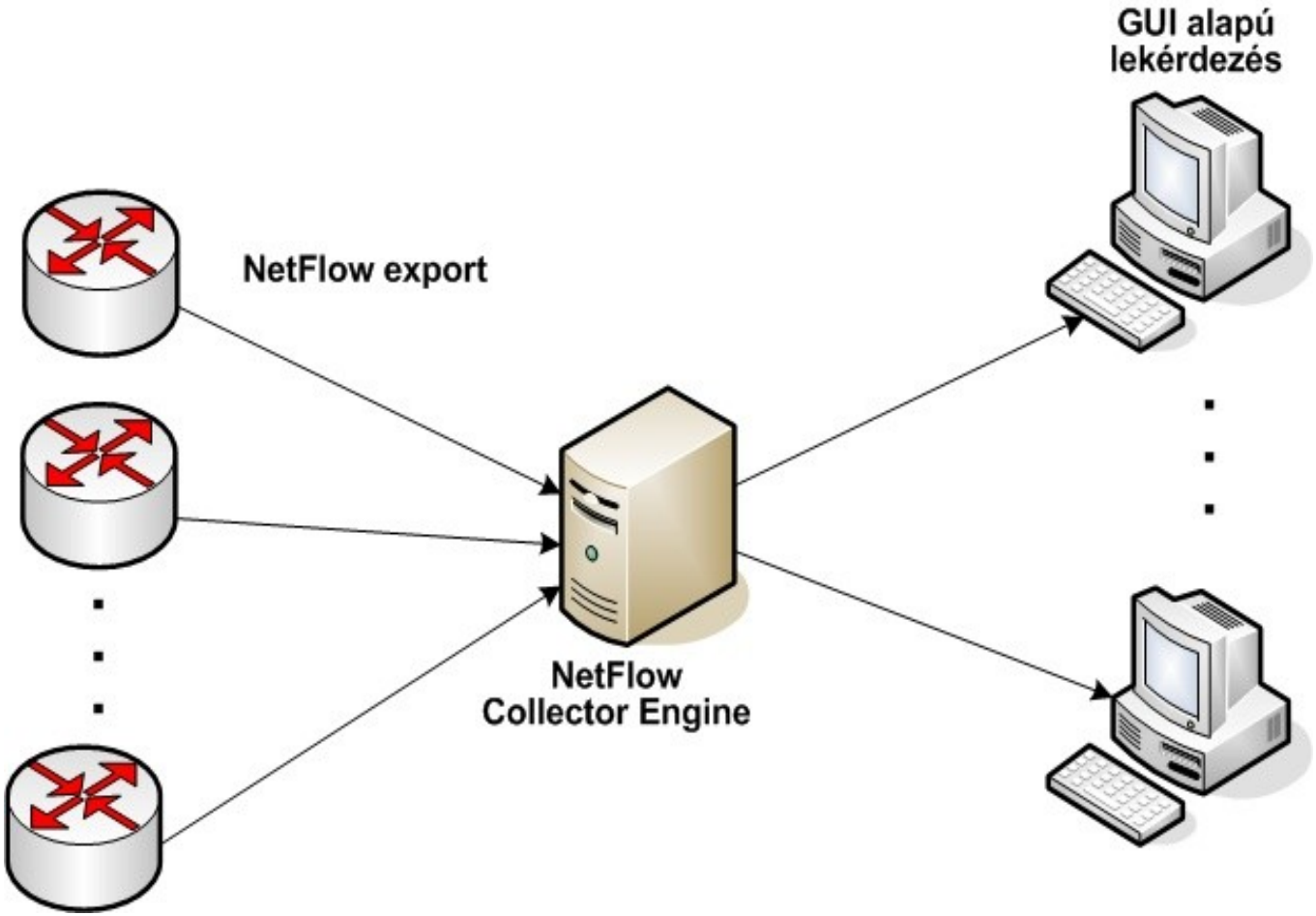
- 1 G+ link
  - könnyen kitölthető, nagyon drága vonalak, teljes monitorozás kérdése
- Erősödő felhordó hálózatok
  - (klasszikus kliens szerver viszony megszűnése, felhasználói szabályzat gyors elavulása
- Átláthatatlan forgalom
  - titkosítások, gyorsan feltűnő és elavuló nem dokumentált alkalmazások
- Pénzért, komolyan dolgozó alvilág, jogvédő szervezetek

Mit tegyünk?

- Forgalom monitorozása (tcpdump, forgalom szétbontása)
- Forgalom szigorú szűrése (proxy, tűzfal stb.)
- Részletes log gyűjtés
- Szigorú felhasználói szabályzatok készítése

- Netflow – Cisco megoldás

Mi az a Netflow?



A “flowk”

- A flowk valamilyen tulajdonság alapján aggregált csomagokról kapott információk.
- A flowk keletkezése:
  1. A Cisco routerek routing táblát építenek fel a csomagok irányításának megkönnyítésére.
  2. A flowk exportálása

Flow tartalom

A flowkban tárolt 7 alap információ:

- Forrás és cél IP címek
- Forrás és cél port számok
- IP protokoll
- Type of Service
- Ingres interfész szám

+ Egyebek

Flow mindig egyirányú!

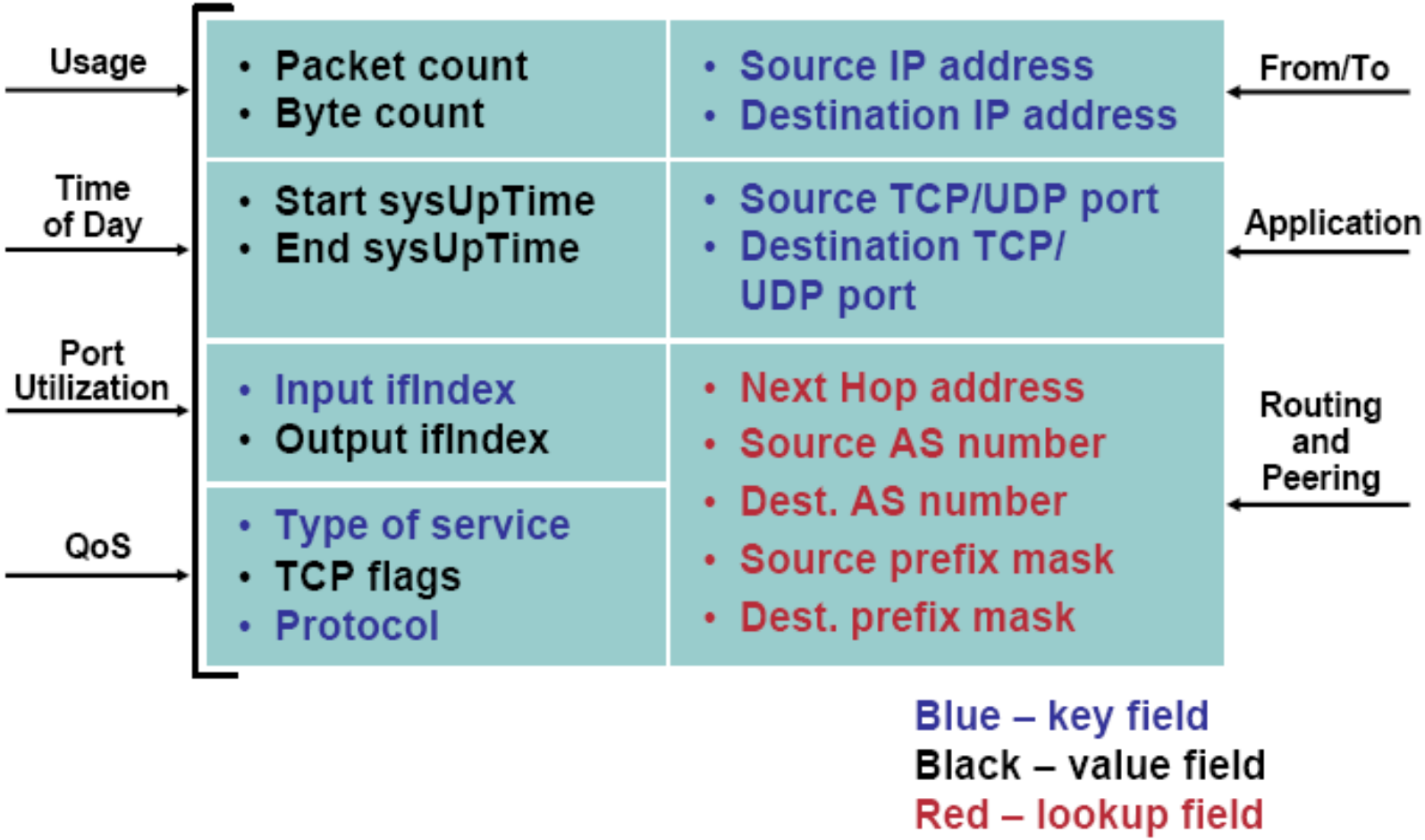
Csak beérkező forgalom! - transit és cél is!

Netflow v5

A flowk tartalma verziótól is függ:

- Netflow V5
  - byte és csomag szám
  - kezdete és vége
  - Kimenő interfész
  - TCP flagek aggregálva
- AS számok(origin,peer), alháló maszk, next hop
- Tulajdonképpen kevesebb is és több is, mint egy header

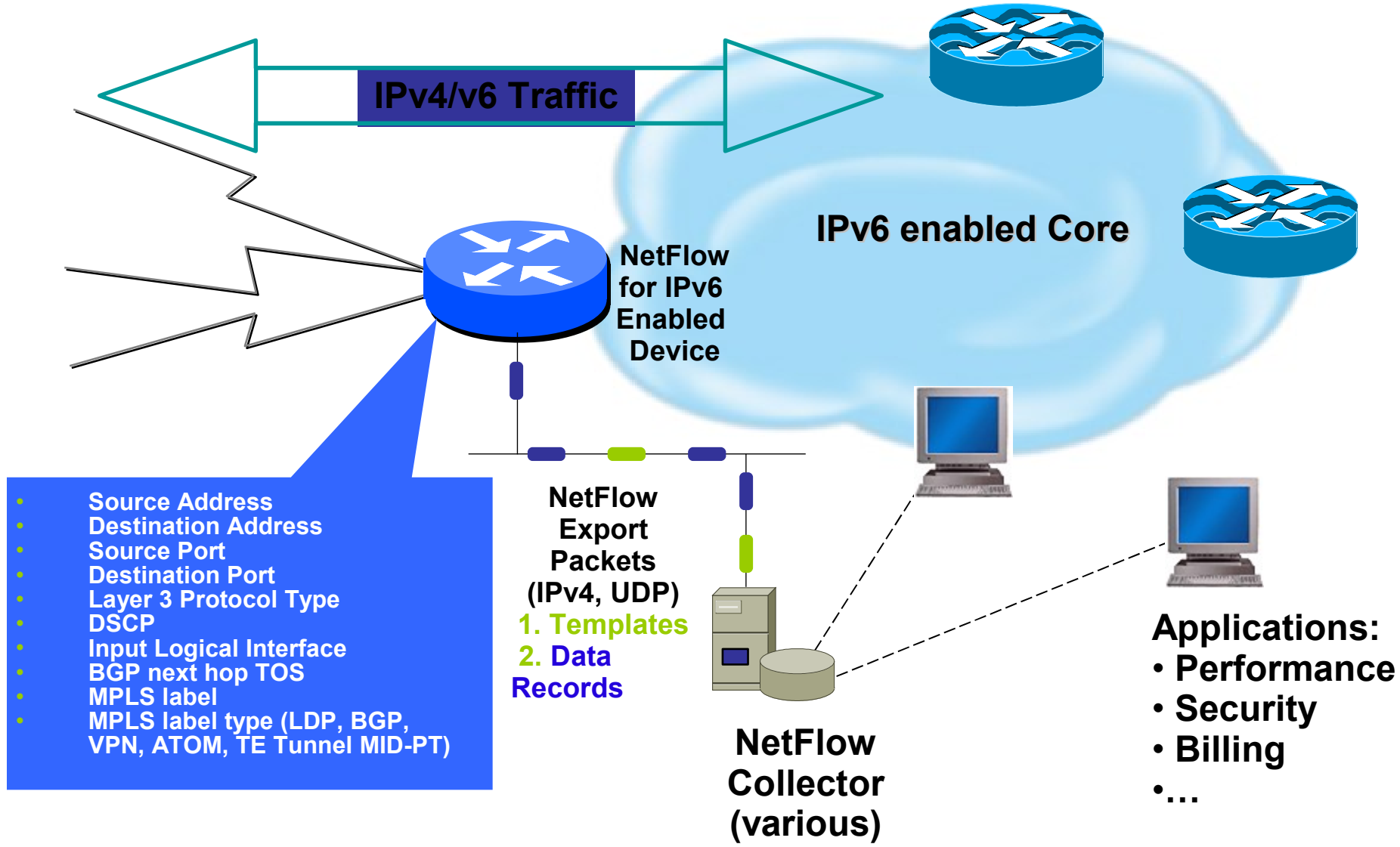
Netflow v5 /2


Usage
Time of Day
Port Utilization
QoS
• Packet count
• Byte count
• Start sysUpTime
• End sysUpTime
• Input ifIndex
• Output ifIndex
• Type of service
• TCP flags
• Protocol
• Source IP address
• Destination IP address
• Source TCP/UDP port
• Destination TCP/ UDP port
• Next Hop address
• Source AS number
• Dest. AS number
• Source prefix mask
• Dest. prefix mask
From/To
Application
Routing and Peering
Blue – key field
Black – value field
Red – lookup field

Egyéb Netflow változatok...

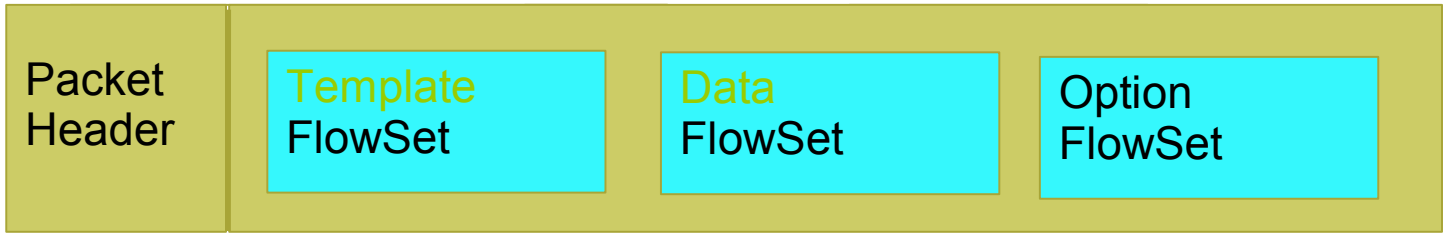
Netflow változat	Leírás
1	Eredeti
5	Leggyakoribb
7	6500 specifikus, mint a v5 de nincsen AS, Interface, TOS és TCP flag
8	Aggregációs sémák
9	Flexibilis NetFlow, MPLS, Multicast, IPv6 stb támogatás

NetFlow v9 és IPv6 támogatás

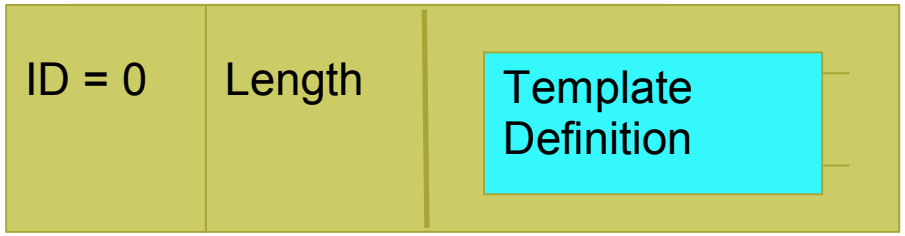


NetFlow Version 9

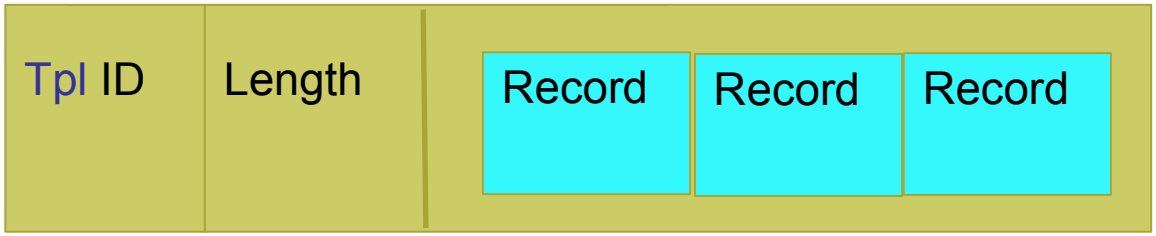
Packet



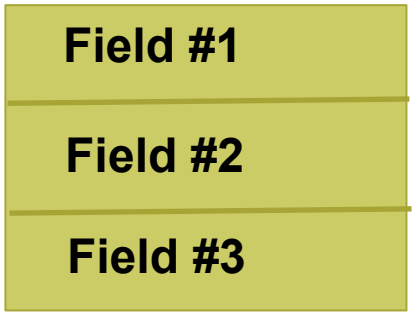
Template Definition (Template FlowSet)



Flow Records (Data FlowSet)



Record

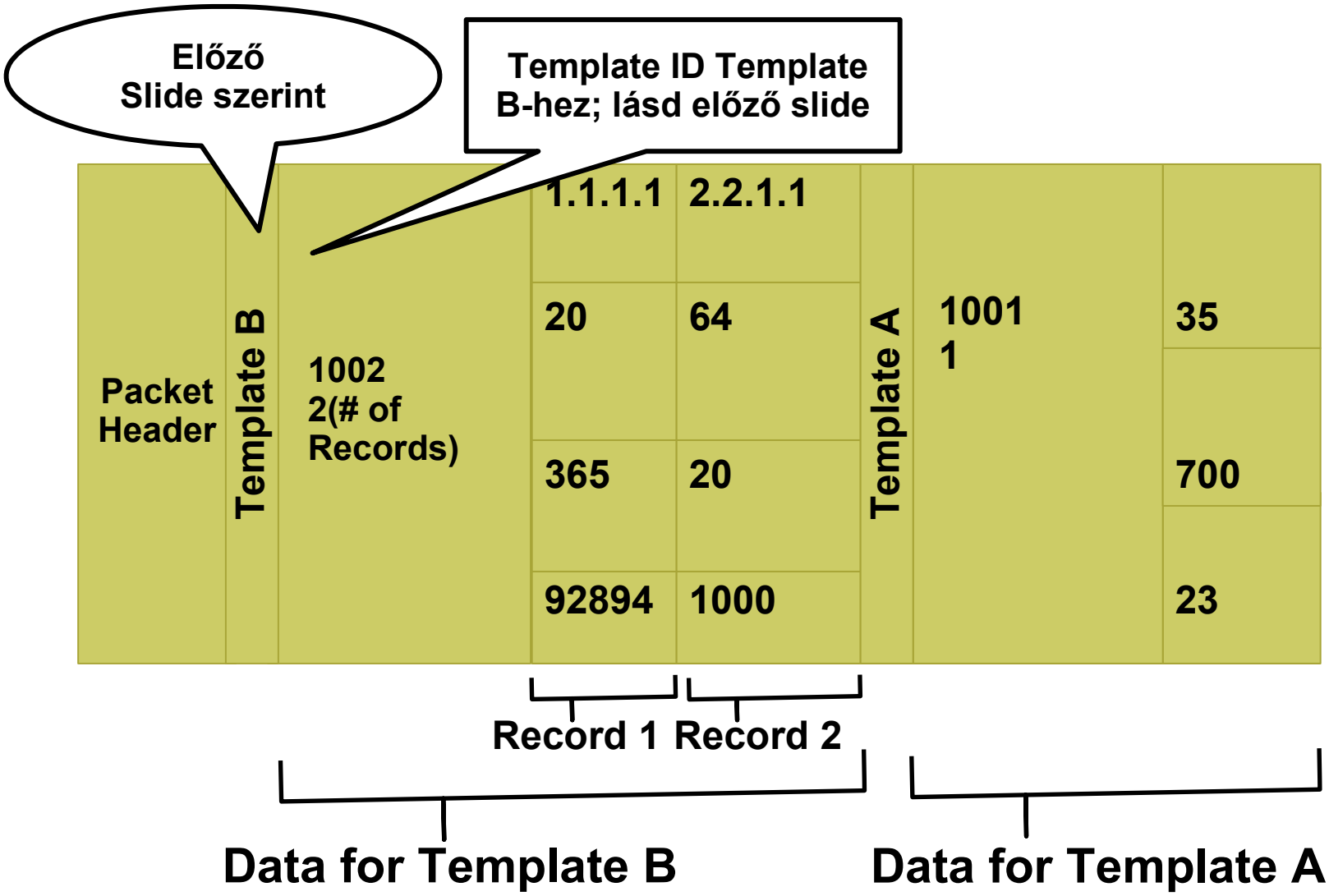


NetFlow Version 9
Példa Template Definition

Template A
Flow Set ID (0 for Template)
Length of Template Structure
1001 (Template ID)
3 (# of Fields)
SRC_AS_NUMBER
2
DST_AS_NUMBER
2
L4_PROTOCOL
2

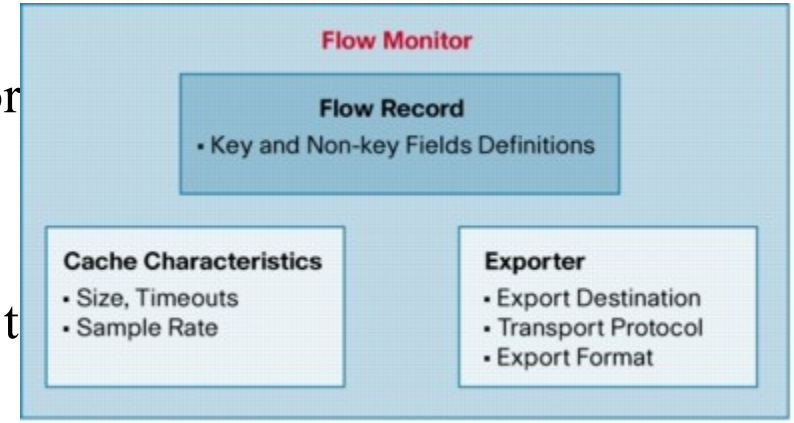
Template B
Flow Set ID (0 for Template)
Length of Template Structure
1002 (Template ID)
4 (# of Fields)
SRC_IP_PREFIX
4
SRC_AS_NUMBER
2
PACKET_COUNT
2
BYTE_COUNT
2

Példa Exportált csomag



IPFIX vs NetFlow v9 és IPv6

- IETF IPFIX WG -IPFIX
  - Majdnem Netflow v9 + további flexibilitás
  - SCTP az elsődleges transzport
  - Privacy
  - Sampling
- Cisco
  - Netflow IPv6 támogatás Cisco IOS 12.3(7)T után
    - Netflow v9-al kompatibilis
    - IPv4 transzport az netflow expor
    - Netflow adatgyüjtők
      - Nerdd, Flowd, NFSen
  - IPFIX támogatás: Flexible Netflow t



Flow támogatás a Cisco-nál

- Támogatott kis routereken:
  - 800, 1700, 2600, 3600, 3700
- Switchek:
  - 4500
- Routerek, NAS-ok:
  - 7200, 7300, 7500, 5300, GSR
- Switching router
  - 6500/7600

Flow Cisco 7200-on

- Subinterface (12.2(14)S vagy 12.2(15)T után)

```
c72.nyhaza(config-subif)#ip flow ingress
c72.nyhaza(config-subif)#
```

- Main interface:

```
c72.nyhaza(config-if)#ip route-cache flow
c72.nyhaza(config-if)#
```

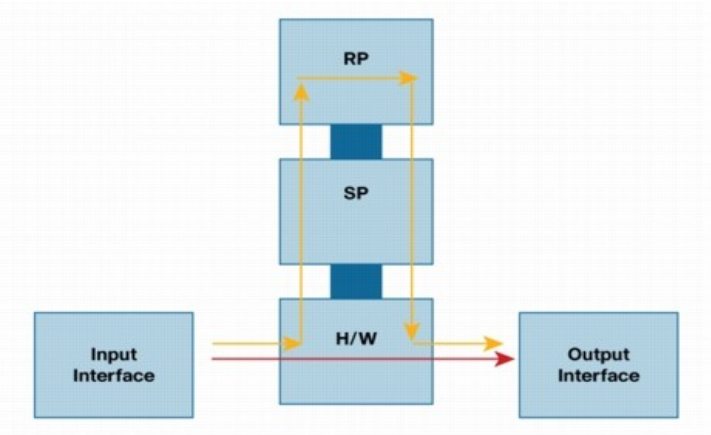
- Export:

```
Router(config)# ip flow-export destination 10.10.10.10 9996
Router(config)# ip flow-export version 5
Router(config)# ip flow-export source loopback 0
```

Flow Cisco 6500/7600-on

- sup720-on nem lehet interfészenként konfigurálni a netflow-t - majd a 12.2(33)SRB? változatban
- Konfiguráció:

```
mls flow ip full
mls flow ipv6 full
mls nde sender v5
```



- 12.2(18)SXE-től kezdve képes a MSFC/SP exportálni - előtte az MSFC/RP másolgatja és exportálja
- 12.2(18)SXF előtt csak v5 utánna v9 export is lehetséges
- 12.2SRB? - interfészenként szabályozható az export.

Flow Cisco 6500/7600-on/2

- Definiálni kell a flowmask-ot:
  - Source: Source IP Address
  - Destination: Destination IP Address
  - Source and Destination: Source and Destination IP Address
  - Interface Source and Destination: Source and Destination IP Address + Input Interface
  - Full: Source and Destination IP Address + Protocol optional TCP/UDP Port Numbers
  - Interface Full: Source and Destination IP Address + Protocol optional TCP/UDP Port Numbers + Input

Flow Cisco 6500/7600-on/3

- DFC-k segítenek a netflow adatok gyűjtésében

	Hybrid	Native 12.1E	Native 12.2SX
MSFCx	v5	v5	v5, v8*
Sup1a	V7, v8	v7	N/A
Sup2	V7, v8	v5, v7	v5, v7, v8
Sup720	v5, v7, v8	v5, v7	v5, v7, v8

*No NetFlow Support on MSFC with Sup1a

Netflow Cisco 4500-on

- NetFlow támogatás Sup4-en
  - 12.1(13)EW támogatja Netflow v5-öt interface tracking nélkül
  - 12.1(19)EW támogatja Netflow v5-öt interface trackingel és Netflow v8-at
- NetFlow támogatás Sup5-ön
  - 12.2(18)EW támogatja Netflow v5-öt és v8-at

Netflow Cisco GSR-en

Engine	Full	Sampled
0	+	+
1	+	+
2	-	+
3	-	+
4	-	-
4+	-	+

Flow a routeren

```
c72.nyhaza#show ip cache flow
...
IP Flow Switching Cache, 4456704 bytes
  9191 active, 56345 inactive, 1324473901 added
  864718286 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 532616 bytes
  9191 active, 23577 inactive, 1324474286 added, 1324473901 added to flow
  0 alloc failures, 0 force free
  2 chunks, 35 chunks added
  last clearing of statistics never
...
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP
   Pkts
Gi0/0.200     12.219.237.164  Gi0/0.10      193.224.106.47  06 1C6D 3EC5
   5
Gi0/0.200     195.228.240.145 Gi0/0.10      193.224.106.45  06 0050 EE3B
   1
Gi0/0.10      193.224.106.44  Gi0/0.200     10.7.190.161    06 94A4 01BD
   1
```

Flow Cache és Export

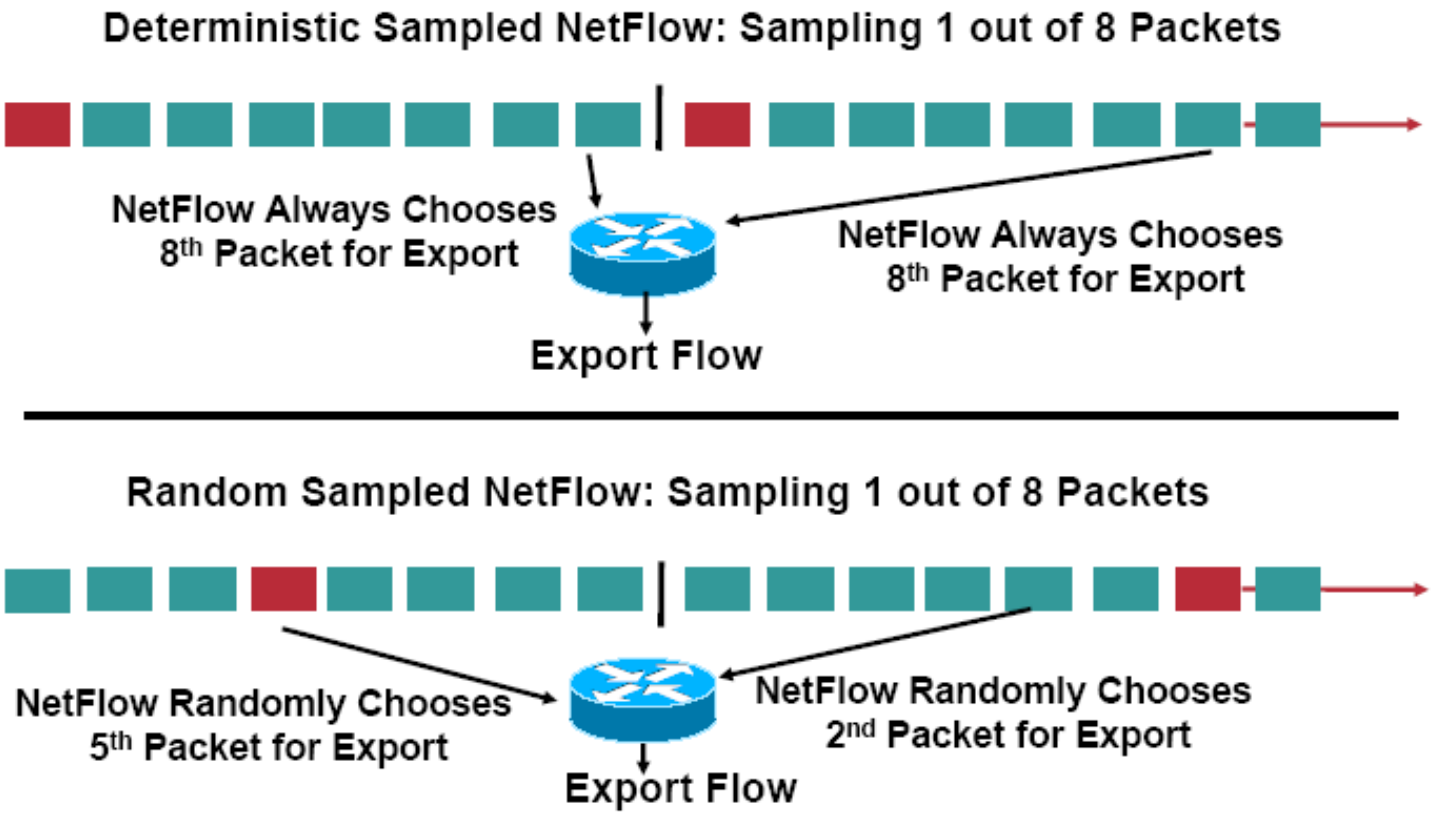
A Cache

- Véges méretű (64-256k)
- 15 s inaktív, 30 m aktív, SYN v. FIN, megtelt cache a flow elévülését okozza

Az exportálás

- Aggregálás(több szempont alapján) – lehet, hogy más netflow formátumot kell használni....
- Sampling (véletlen, meghatározott; kevesebb erőforrás, de adatvesztés)

Netflow sampling



Flow exportálás konfiguráció

- `ip flow-export destination <address> <port>`
  - pl. ip flow-export destination 10.0.0.1 65001
- `ip flow-export source <interface>`
  - Default interfész- ha szűrés van, vagy meghatározott irányt szeretnénk konfiguráljuk
- `ip flow-aggregation cache <name of aggregation scheme>`
  - Aggregációs cache választás
- `ip flow-cache timeout inactive <seconds>`
  - Inaktív flow-k ennyi ideig maradnak a cache-ben. Default 15 másodperc
- `ip flow-cache timeout active <minutes>`
  - Aktív flow-k ennyi idő után biztos exportálodnak. Default 30 perc
- `ip flow-cache entries <number>`
  - Sets the maximum number of flow entries in the cache. The default varies dependent on platform.

Flow show/clear commandok

- `show ip cache [verbose] flow`
  - NetFlow cache megnézése
- `show ip cache flow aggregation` `<name of aggregation scheme>`
  - Adott aggregációs cache megtekintése
- `show ip flow export`
  - Export statisztikák megtekintése
- `clear ip cache flow`
  - NetFlow cache törlés
- `clear ip flow stats`
  - Export statisztika törlés
- sh mls netflow table-contention aggregate |summary
  - Cisco 6500/7600 tábla használat

Flow újabb dolgok

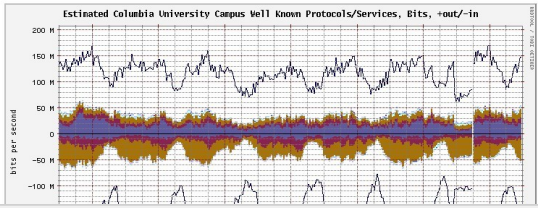
- `show ip flow top (12.4T)`
  - Egy bizonyos mintára illeszkedő legtöbbet “beszélő” (byte vs csomag) ip címek aggregálva
- `show ip flow top-talkers (12.3(11)T)`
  - Egyedi legtöbbet beszélő flow
- Detektáláshoz hasznos (12.4(2)T után)
  - `ip flow-capture {icmp | ip-id | mac-addresses | packet-length | ttl | vlan-id}`
- Multicast (12.3(1) után)
  - `ip multicast netflow {ingress | egress}`

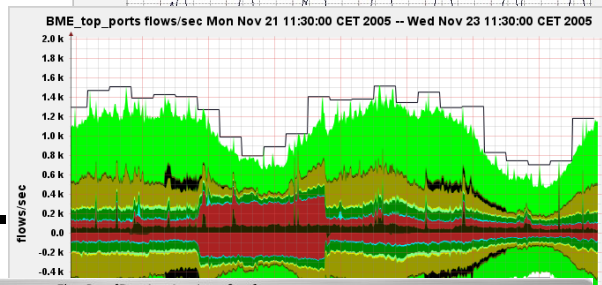
Netflow teljesítmény igény

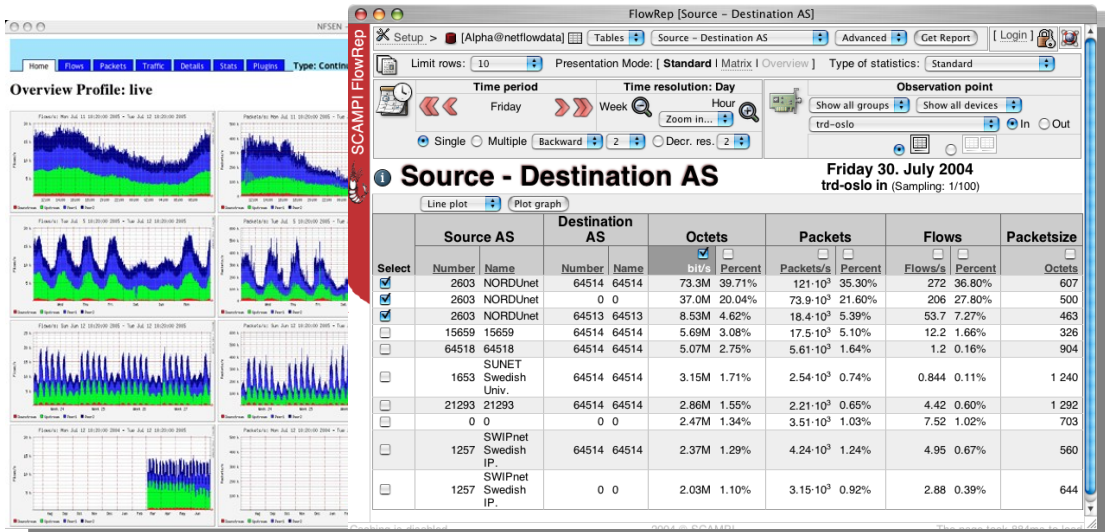
- Forgalom <1%-al növekszik az exportálás miatt
- Cisco 7200:
  - Netflow v5/v9 engedélyezés kb. 4-16% CPU többletet igényel (sok flow-nál többet)
  - v5- 64 byte-ot igényel pluszban flownként: 64000 flow ~ 4MB RAM
- Cisco 6500- sup720
  - Gyűjtés nem igényel további CPU erőforrást, de TCAM erőforrást igen! - DFC-nél nem
  - Exportálás (pre SXE) 35-40%, post SXE(16%/export)

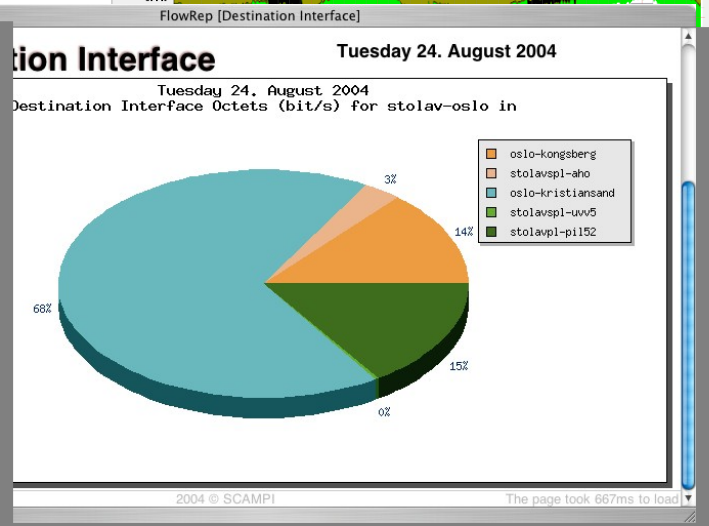
Netflow collectorok

- Néhány példa a szoftverekre http://www.switch.ch/tf-tant/floma/software.html:
  - Flowscan, flow-tools, nfdump..
  - Cuflow, Stager...
  - Mégtöbb script...
  - És rengeteg fizetős szoftver..





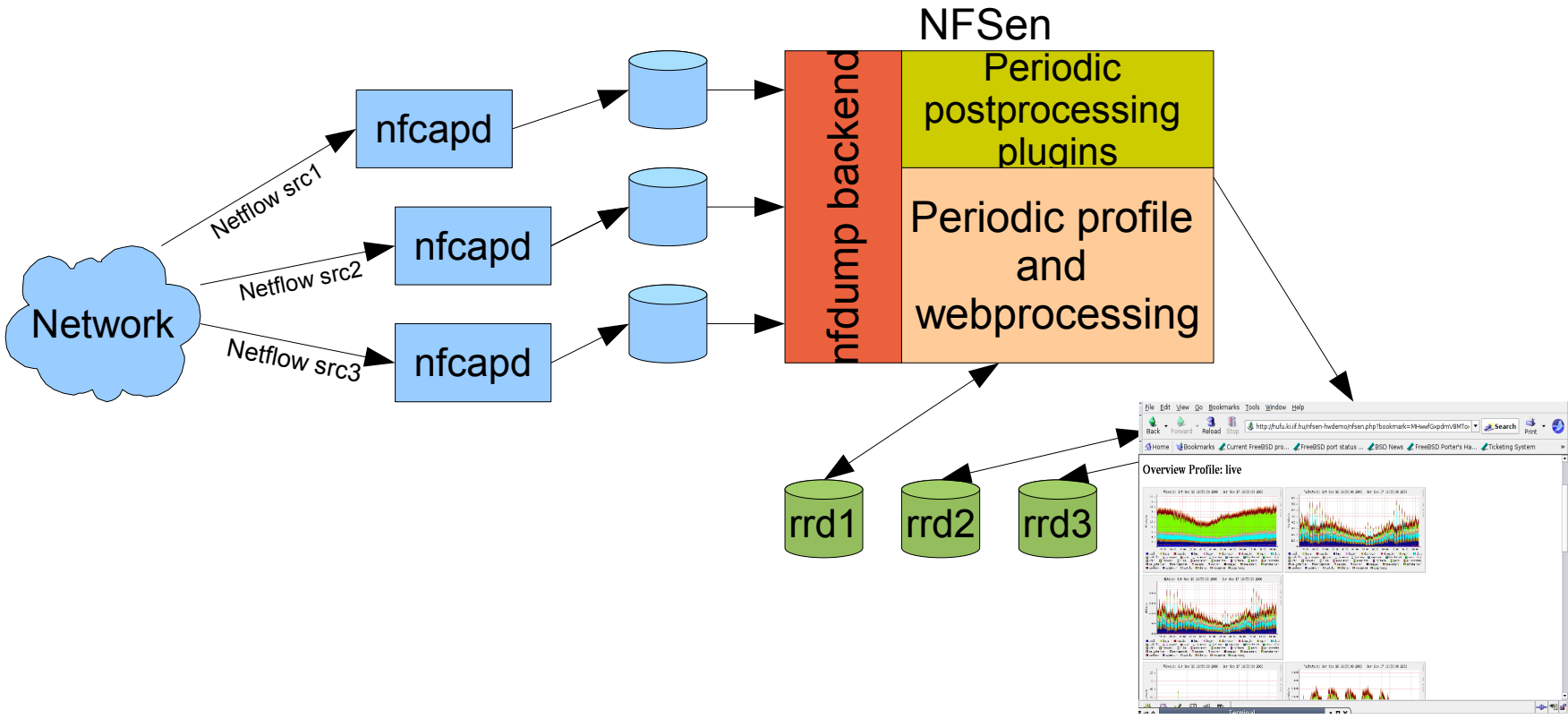




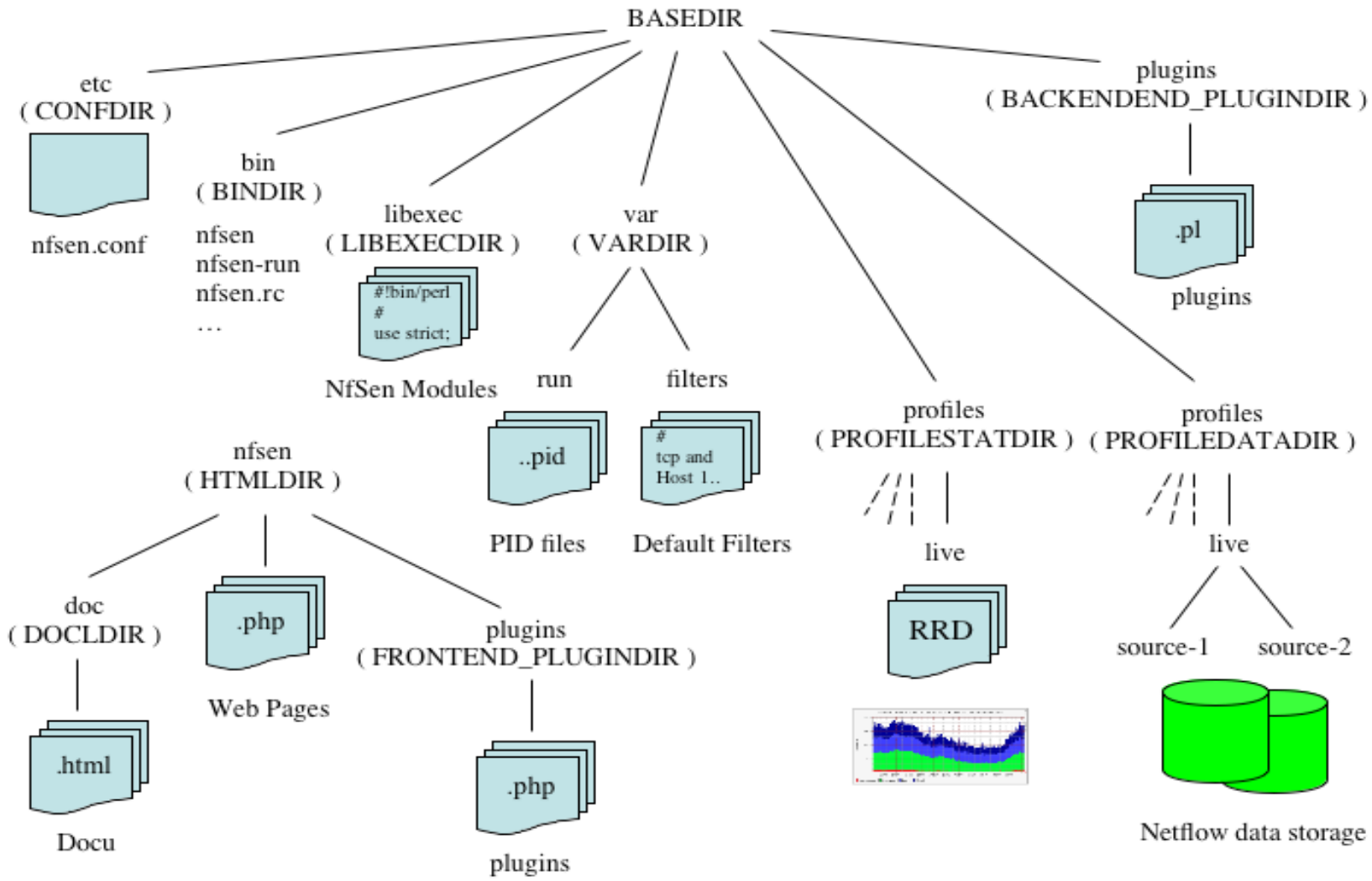
NFSen és nfdump

- SWITCH - svájci NREN
- NfDump + NfSen
  - Gyors – amíg nem kell statisztikát gyártani
  - Nagyon egyszerű – könnyű eligazodni benne
  - Könnyű használni (persze lehet hozzá írogatni...)
  - Könnyű navigáció, gyors ábrák
  - Egyszerűen létrehozható statisztikák
  - Sok, sok, sok diszk igény

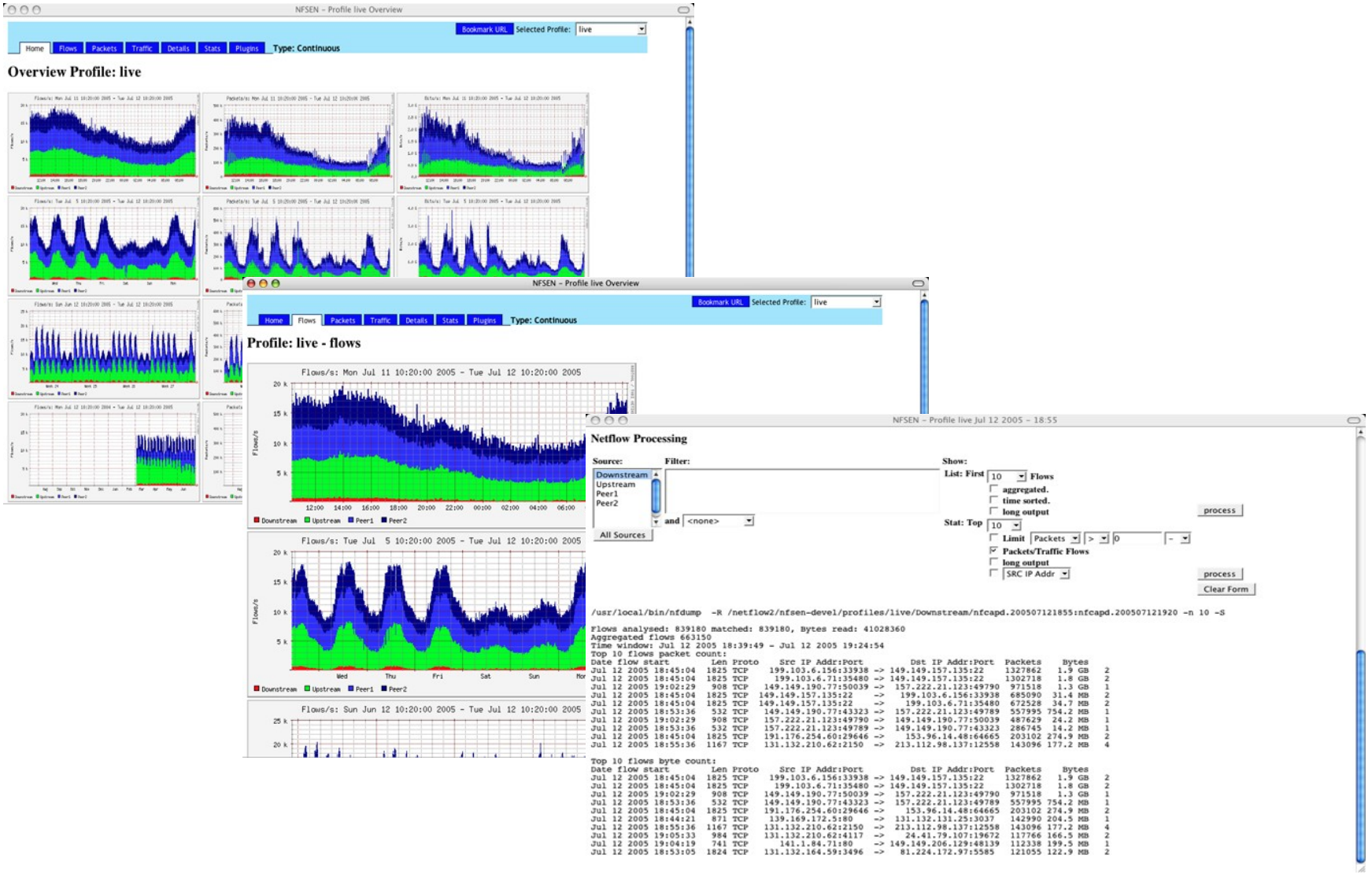
NfSen/nfdump architektúra



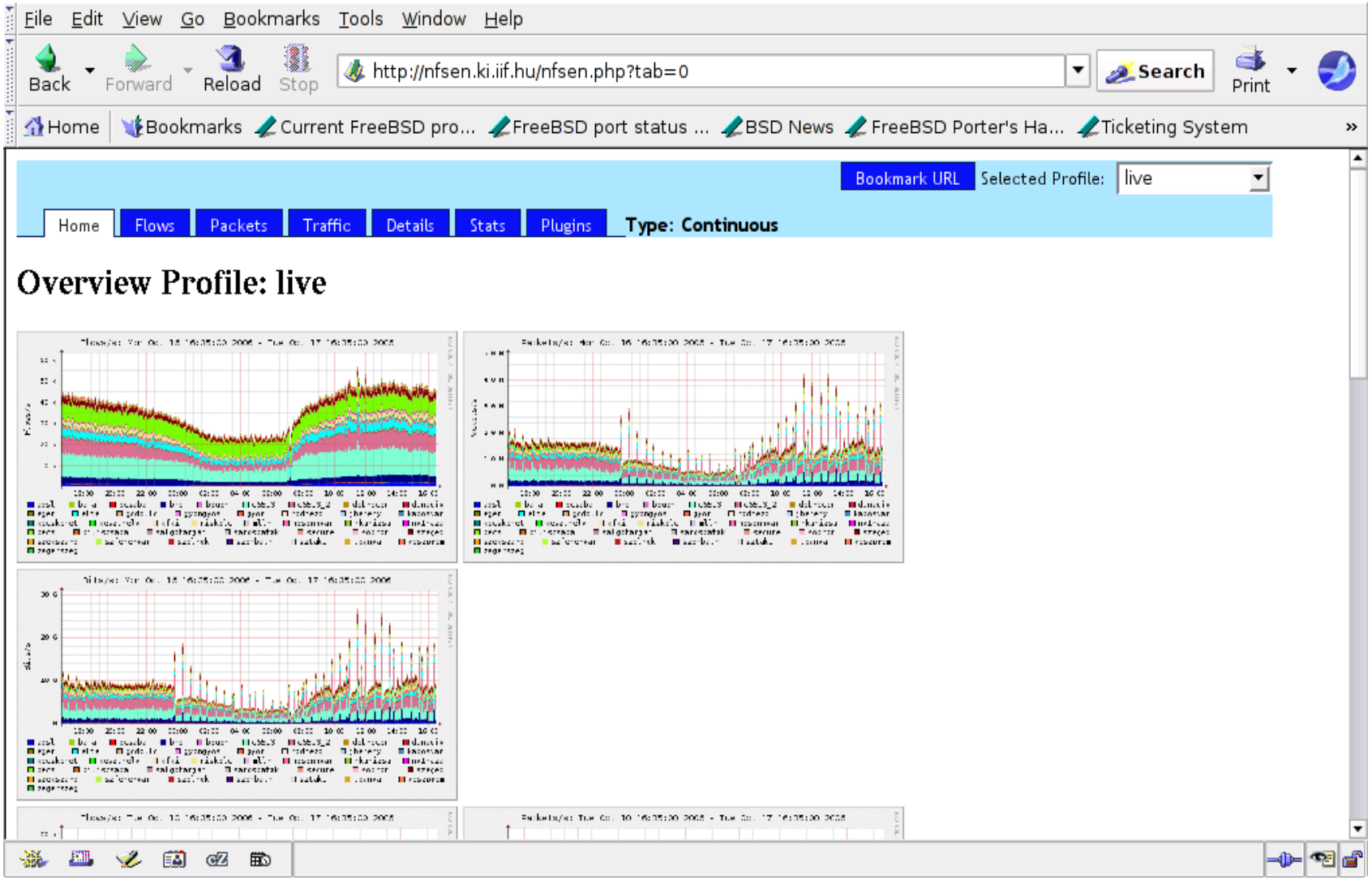
NFSen könyvtár struktúrája



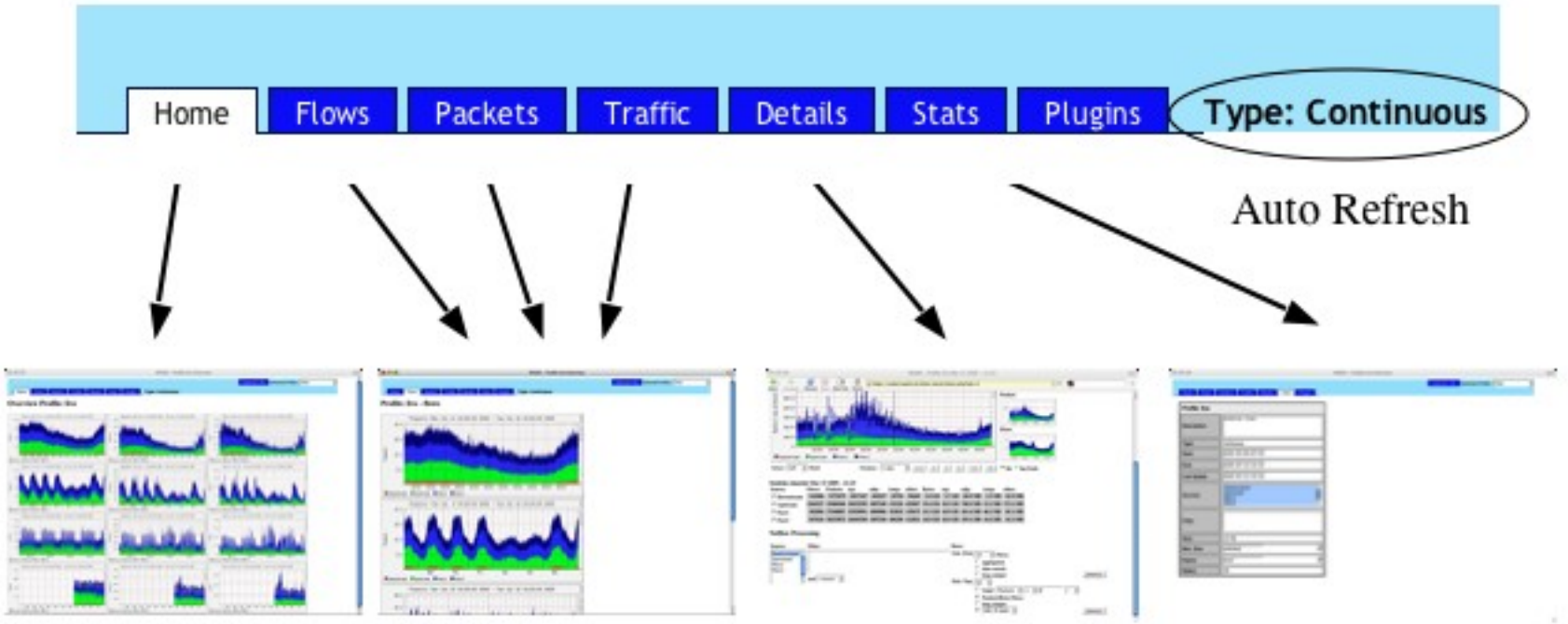
NFSen Netflow kimenet



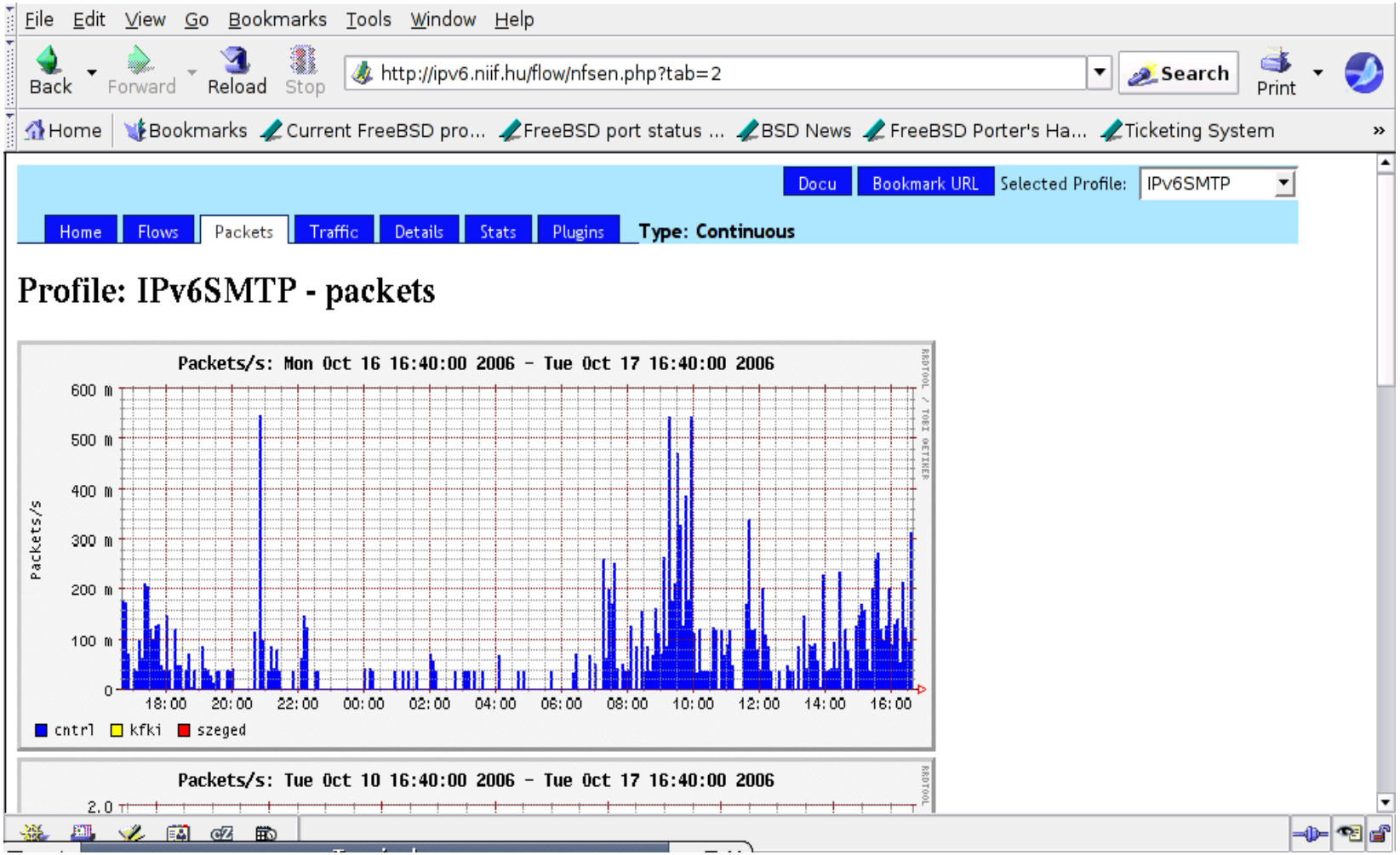
NFSen kezdőképernyő



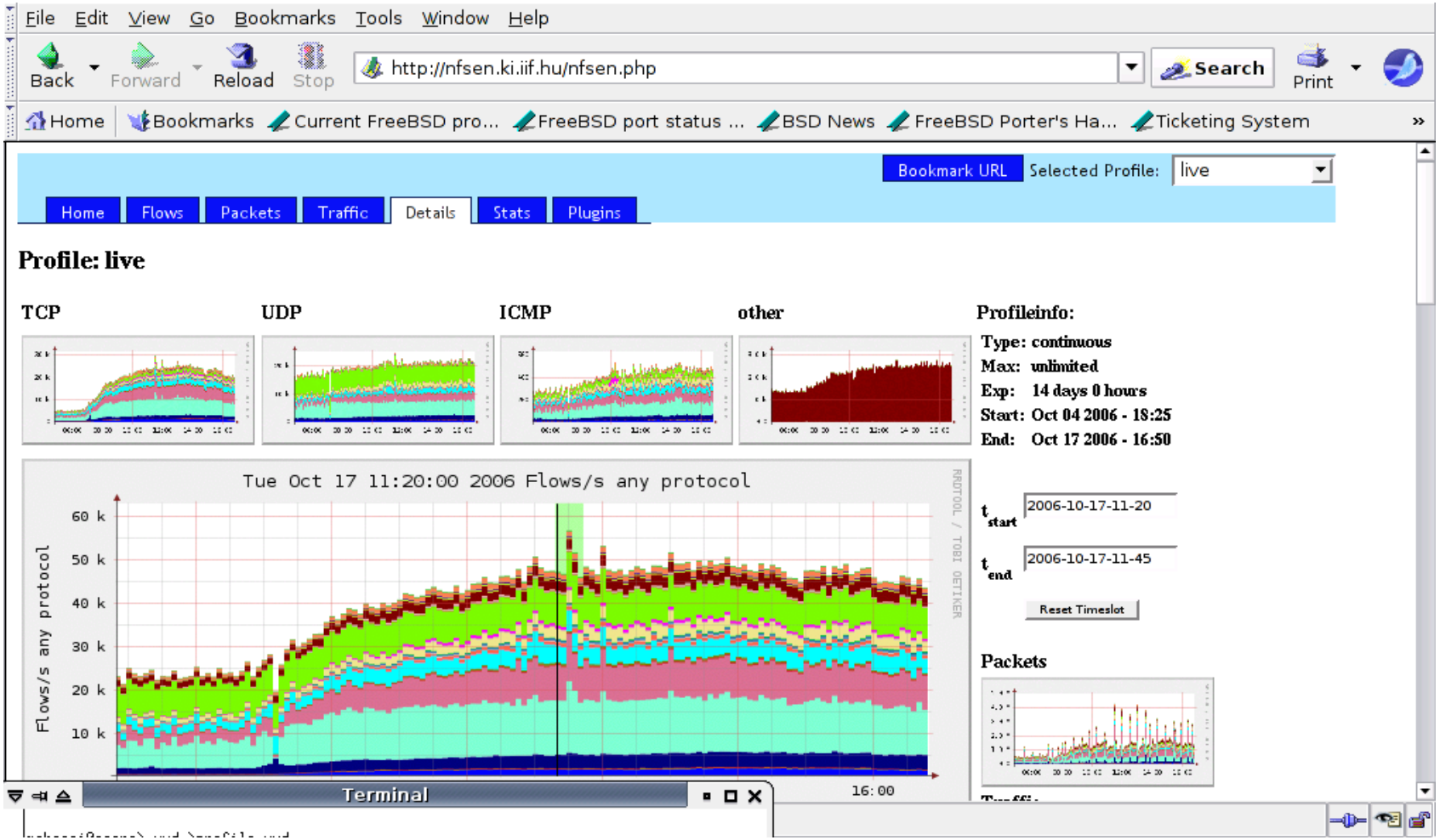
NFSen navigáció



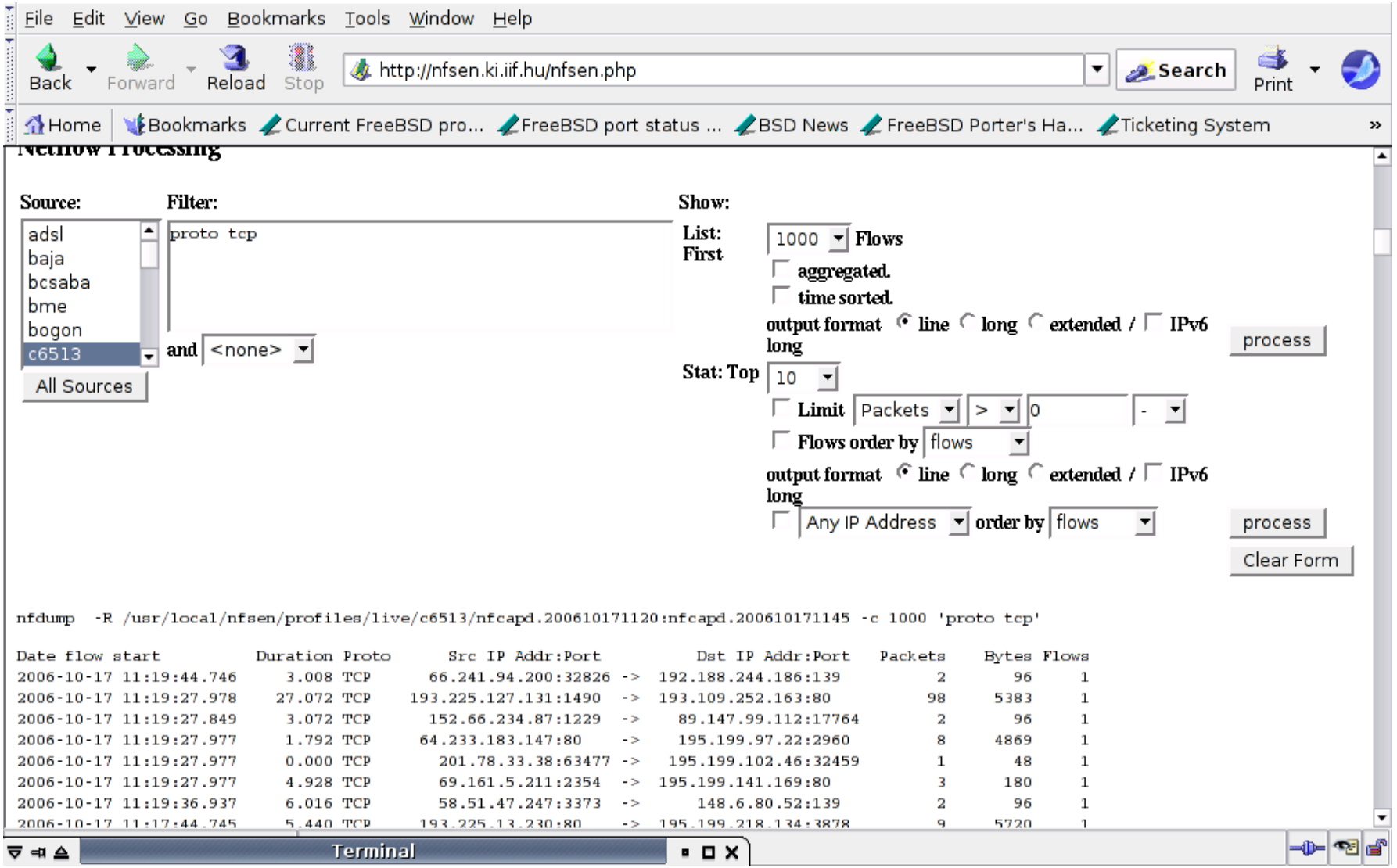
Adott tipusú forgalom - profileok



Szénakazal széttúrás



Mi is történt?



NFSen, nfdump parancssori interfész /1

- nfcapd – hálózatról érkező netflowk letárolása
- nfreplay – flow tovább küldése
- nfprofile – profile szerinti szűrés
- ft2nfdump – flow-tools to nfdump formátum konverter
- nfdump – általános szűrő mint a tcpdump

NFSen, nfdump parancssori interfész /2

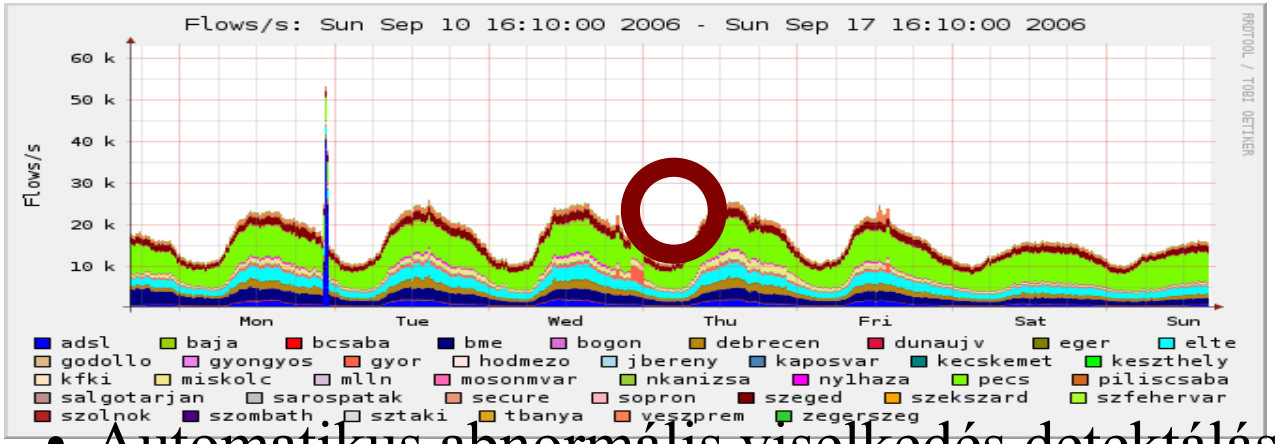
- Az `nfsen.rc` elindítja:
  - `Nfcapd`, nfprofiler 5 percenként
  - `Nfsen-run` , 5 percenként (grafikonok)
- `Nfsen`
  - Profilok kezelésére
    - Profilok létrehozása, törlése, újraépítése, módosítása, kilistázása
  - Ha a webes interfész valami miatt nem működne
- `Nfsen-run`
  - Rendszeresen futó (5 perc)
  - `Nfsen-run once` – ha nem használnánk az `nfsen.rc` -t

NFSen bővítés

- Pluginok
  - Backend plugin
    - Perl module
    - Nfsen-run indulásánál fut le (5 percenként)
    - Az nfdump-ot használhatjuk, kimenetét dolgozhatjuk fel
    - példa:demoplugin.pm, Notification.pm
  - Frontend plugin
    - Backend plugin megjelenítésére
    - php kód
    - Példa:

Mi az amit nézzünk?

- Biztonsági csoport mit csinál:
  - Abnormális viselkedés keresés
    - Csúcsok vizuális detekciója

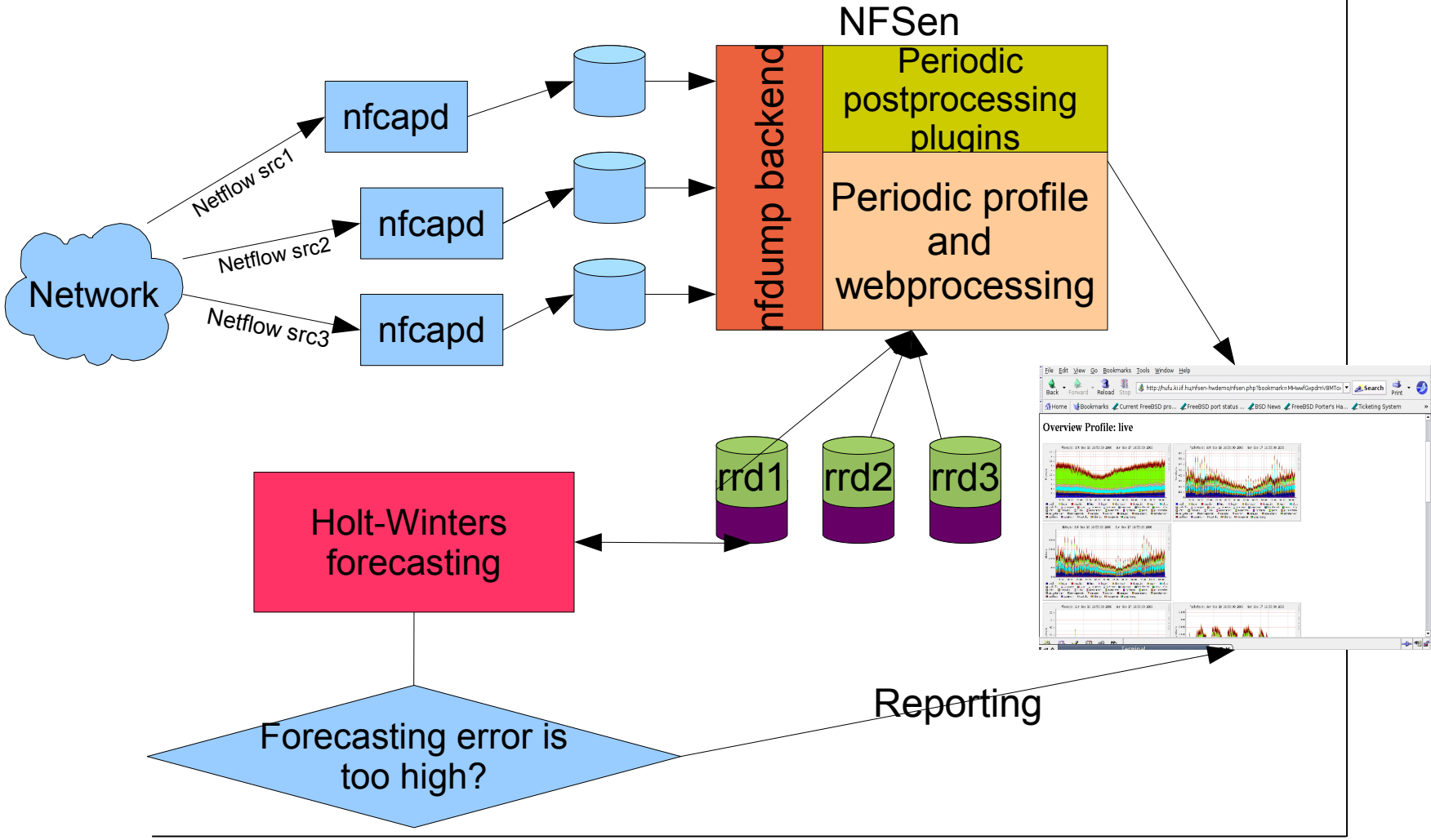


    - Automatikus abnormális viselkedés detektálás- meg tudjuk mondani mi az abnormális?
  - Incidens koordináció
  - Segítség a vizuális anomália detekcióhoz

Anomália detektálás

- Megfigyelés:
  - A forgalmi/flow viszonyok heti periodicitást mutatnak – növekvő forgalom mennyiséggel
  - Az abnormális flow növekedés (DDoS, Scan) detektálható ha a statisztikus adatoktól eltérés tapasztalható
  - A netflow adatok újra feldolgozás túl nagy feladat volna – Nfsen (nfdump) már elkészítette a feldolgozást és az eredményeit RRD adatbázisba tette
- Szükséges: Előrejelző rendszer, amely képes statistikusan előrejelezni szezonális és trenddel rendelkező viselkedés
- Riasztás: ha az előrejelzett és a mért nagy mértékben eltér

Architecture of NfSen/nfdump with Holt-Winters forecasting

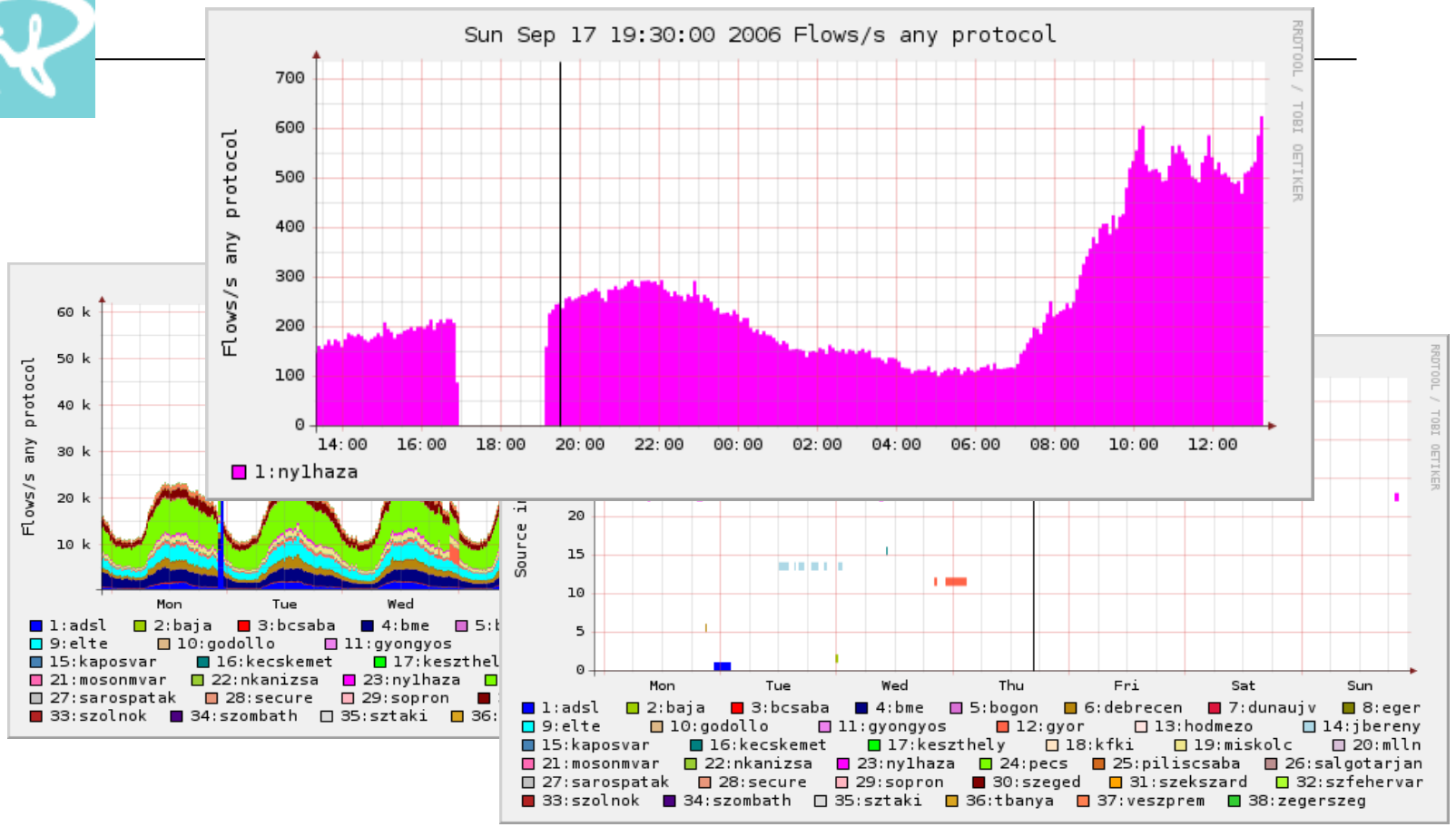


Az RRDTool Holt-Winters implementációja

- Minden számított paraméter RRA-ban tárolódik:
  - HWPREDICT – Holt-Winters előrejelzés – minden adatponthoz
  - SEASONAL – periodicitási együttható – minden adatponthoz
  - DEVPREDICT – eltérési paraméter
  - DEVSEASONAL – szezonális eltérési paraméter
  - FAILURES – logikai értékek

Az RRDTool Holt-Winters implementációja/2

- Új paraméter rrdtool create-nek – egyszerűsített interfész:
  - RRA:HWPREDICT:<array length>:<alpha>:<beta>:<period>
- Új paraméterek tune-nak:
  - alpha, beta, gamma, positive/negative confidence interval, failure treshold megadására



- Elkülönített RRD – teszt célból
- Intuitivebb interfész – külön anomália diagram – 2 click
- Képes detektálni az anomáliat, akkor is ha nem látható

Jövő

- Problémák –
  - α, β és γ Van itt önként jelentkező statisztikus?
  - Periodicitás napi/heti ?
  - Legalább egy hét tanulás szükséges mielőtt érdemben tudna jósolni – és abnormális müködést detektálni
  - Mi is az amit detektálunk? - van más fajta fontos abnormalitás?

További információk

- Matematika:

  http://www.itl.nist.gov/div898/handbook/pmc/section4/pmc435.htm

- RRDTool implementáció (J. Brutlag):

  http://cricket.sourceforge.net/aberrant/rrd_hw.htm

  http://www.usenix.org/events/lisa2000/full_papers/brutlag/brutlag_html/

- NFSen HW implementáció:

  http://bakacsin.ki.iif.hu/~kissg/project/nfsen-hw

Köszönetek: Cisco, Zeisel Tamás, CampusIPv6 projekt, GN2

?

net-admin@niif.hu