PV210 Bezpečnostní analýza síťového provozu

Úvod do bezpečnostního monitorování sítě

Tomáš Jirsík

15. 10. 2014

Motivace

SNMP

Syslog

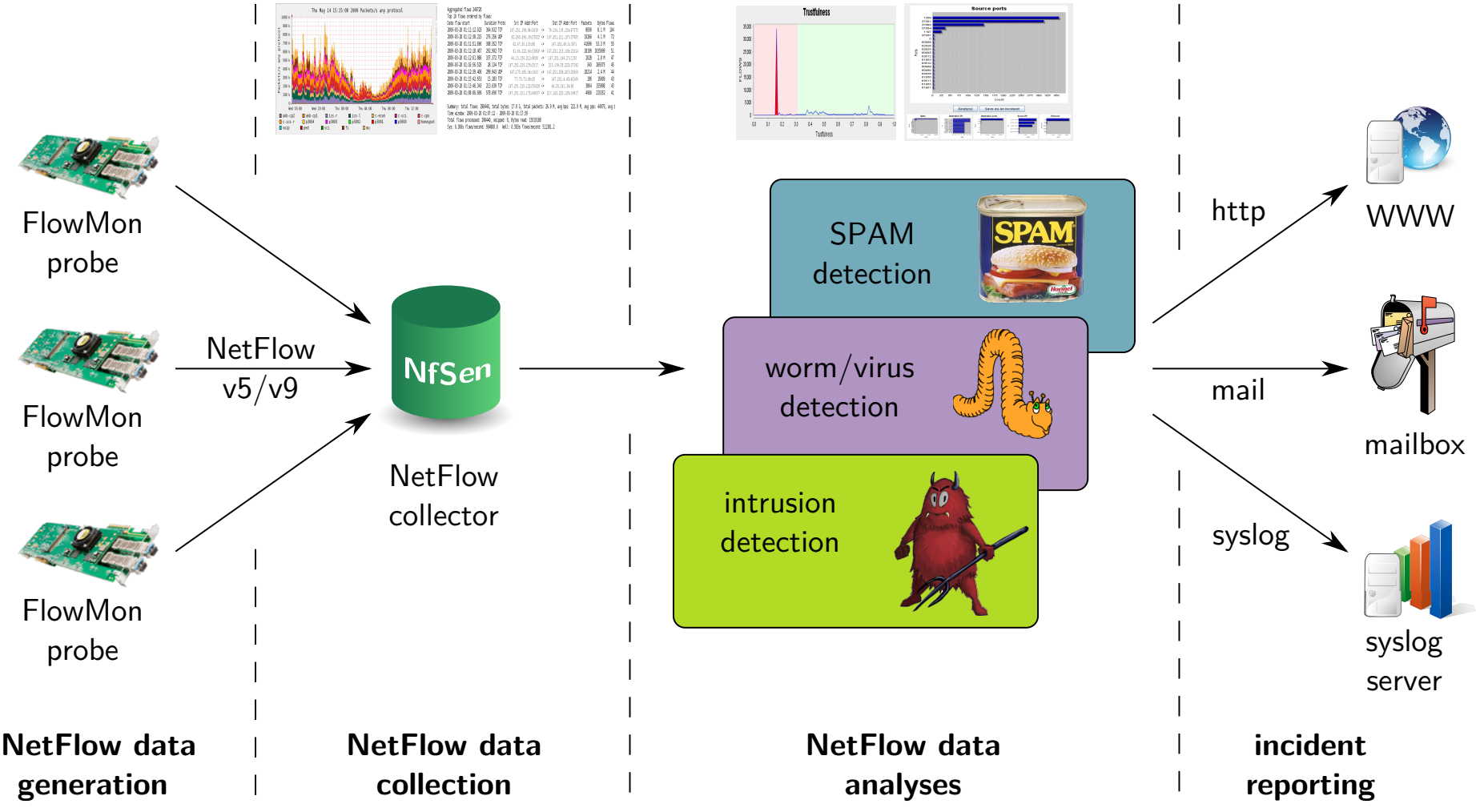
NetFlow, IPFIX

Jak dobře znáte svoji síť ?

- Víte o tom, co se děje ve Vaší síti?
- Jste si jistí bezpečností Vaší sítě?
- Znáte kritická místa Vaší sítě?
- Vypořádáváte se s problémy ve Vaší síti?

A nebo Vám v síti řádí neznámí skřítci?

Architektura systému



Simple Network Management Protocol

- Základní nástroj pro monitorování sítě.
- Viz RFC 3411–RFC 3418, SNMPv3 je standardem IETF od roku 2004.
- Na straně *managed device* se o komunikaci stará *agent* (softwarový démon), který předává informace *manažerovi*.
- Zabezpečení přístupu: *SNMP communities* (read-only, read-write).
- SNMPv3 přináší integritu zpráv, autentizaci a šifrování.

SNMP – dva režimy

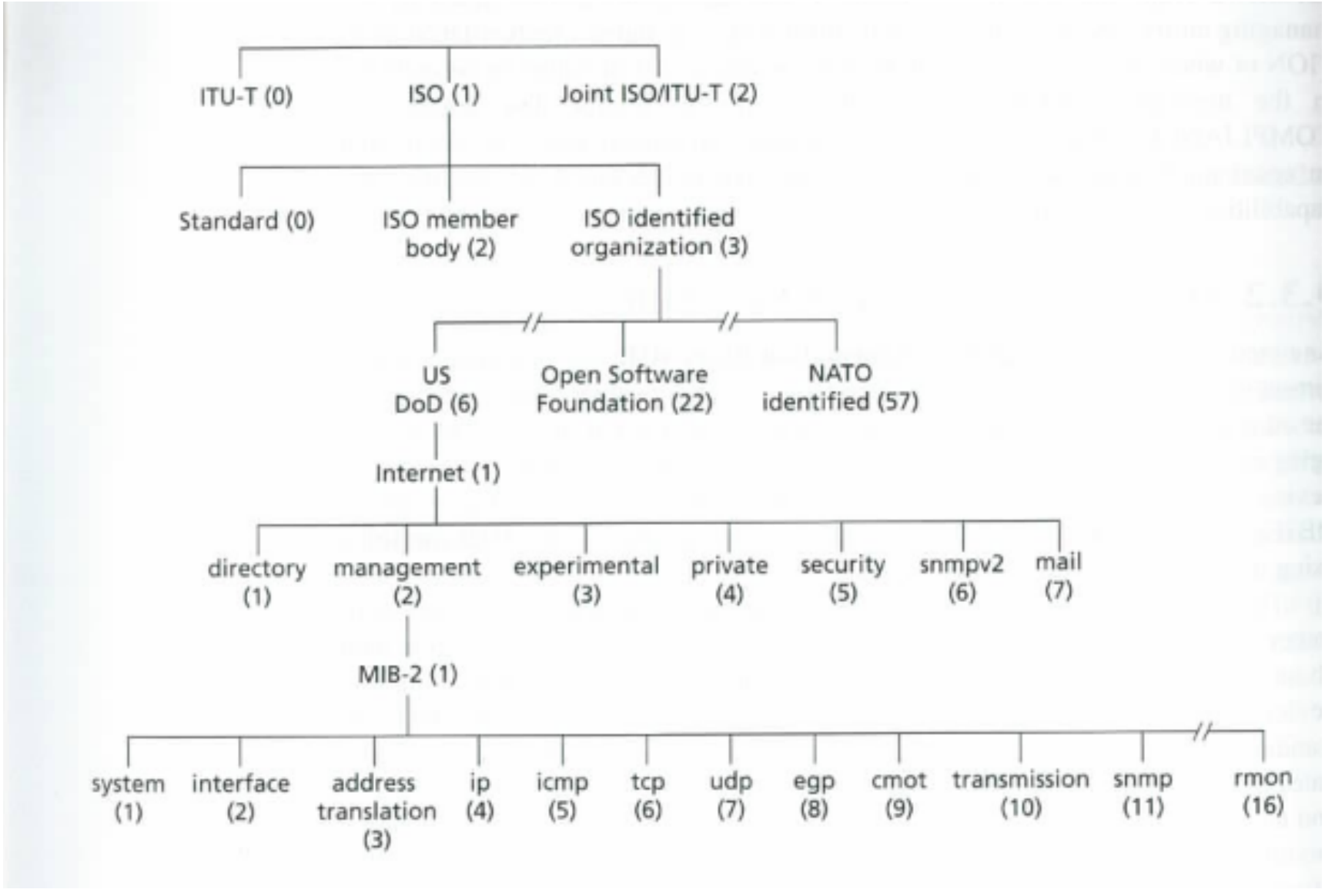
- Dotaz–odpověď: manažer požádá agenta o určitou akci, ten ji provede (nebo také ne) a pošle odpověď.
- *Trap*: asynchronní zpráva generovaná agentem, který manažera upozorňuje na změnu stavu zařízení nebo nějaký jev.

Management objects aneb co lze monitorovat

- Každý objekt reprezentuje konkrétní údaj (konfigurační parametr, statistiku, ...) nebo jejich posloupnost.
- Soubor (databáze) objektů se nazývá *Management Information Base* (MIB).
- Objekty (OID) jsou dále tématicky členěny (podle typu zařízení nebo služby apod.) do MIB modulů.
- Příklad OID: 1.3.6.1.2.1.2.2.1.11 = ifInUcastPkts[1]

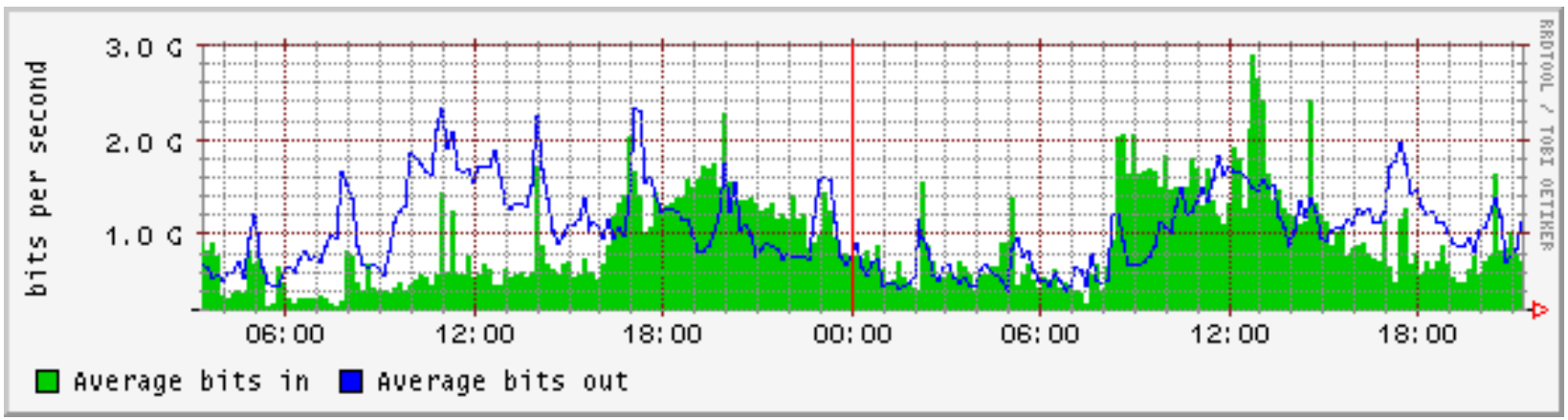
[1] The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.

Struktura MIB



Software pro SNMP I

- MRTG (Multi-Router Traffic Grapher)
  `http://oss.oetiker.ch/mrtg/`



Software pro SNMP II

- Net-SNMP
  `http://www.net-snmp.org`
- Nagios
  `http://www.nagios.org`
- Zabbix
  `http://www.zabbix.com/`
- Cacti
  `http:///www.cacti.net/`

Syslog

- V Linuxu (de facto) standard pro lokální i vzdálené logování (prvopočátek v 80. letech - sendmail).
- Široce používaný protokol napříč platformami a různými typy zařízení.
- Opět popsán v několika RFC, poslední RFC 5424 je z března 2009.
- Klient odesílá serveru krátké zprávy v čitelné podobě (typicky jako UDP datagramy). Např.:

  ```
  Nov 5 14:38:22 medea kernel: [443050.645716] wlan0: authenticated
  Oct 18 12:11:56 ariel sshd[3135]: Failed password for invalid user test
  from 116.32.195.44 port 34026 ssh2
  ```

- Existuje řada implementací, více v BP Karla Hromka (archiv prací v IS MU).

Pasivní vs. aktivní monitorování sítě

Pasivní monitorování

- Do sítě nijak aktivně nezasahujeme.
- Pasivně odposloucháváme síťový provoz, sledujeme statistiky skutečného provozu.
- Příklad: SNMP, NetFlow, IPFIX aj.

Aktivní monitorování

- Do sítě posíláme testovací pakety a sledujeme reakci sítě.
- Příklad: ping, traceroute.

Sběr a analýza paketů

- Tradiční IDS (např. Snort) provádí analýzu obsahu paketů.
- Už v gigabitových sítích není možné provádět tuto operaci v reálném čase bez podpory specializovaného hardware.
- Off-line analýza není možná: vysoké nároky na úložiště (velké objemy rychle přibývajících dat), neaktuálnost výsledku.
- Proto se zavádí určitý kompromis: sběr a následná analýza statistických informací o síťovém provozu.

Síťové toky – definice

Definice z RFC 3954 (Cisco NetFlow Export Version 9)

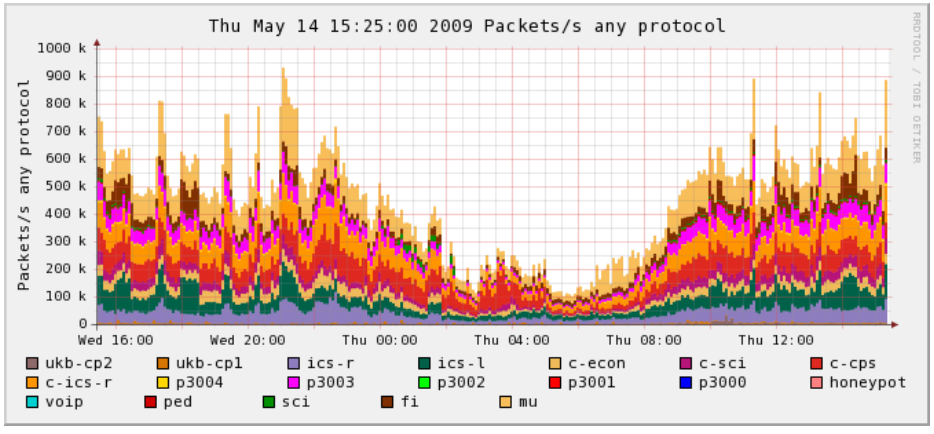
A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc.

IETF IPFIX RFC

- RFC 7011 - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information
- RFC 7011 – 7015 - Kompletní sada IPFIX specifikací

Monitorování toků

- Poskytuje informace o tom kdo, s kým a jak dlouho komunikoval, kolik přenesl dat a jaký protokol použil.
- Základní technologie jsou NetFlow v5/v9 a IETF IPFIX.
- Umožňuje dlouhodobě sledovat síťový provoz v reálném čase.



Detailní pohled do sítě na základě NetFlow a IPFIX dat.

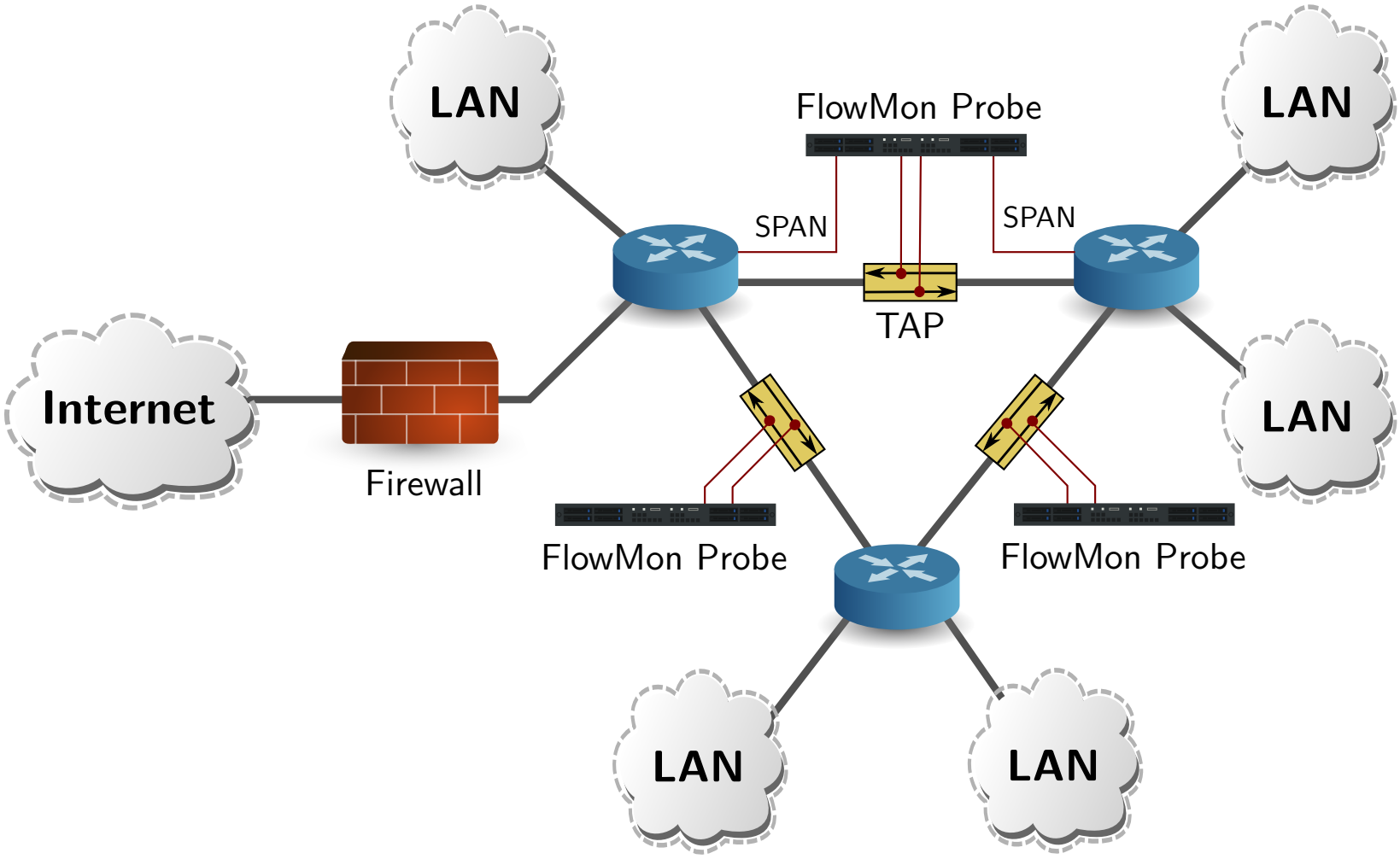
Síťové toky – Princip monitorování toků

Flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Packets	Bytes
09:41:21.763	0.101	TCP	172.16.96.48:15094	->	209.85.135.147:80	.AP.SF	4	715
09:41:21.893	0.031	TCP	209.85.135.147:80	->	172.16.96.48:15094	.AP.SF	4	1594

Síťové toky a agregace

- Toky představují střední úroveň agregace, na vysokorychlostních linkách ale i tak generují velký objem dat.
- Příklad: pětiminutový vzorek dat z mezinárodní 10GE linky do GÉANT2:
  - 578 944 960 bajtů
  - 6 163 012 paketů
  - 152 010 toků
  - 45 284 různých párů IP adres
- Počet toků závisí na parametrech sběru toků:
  - *inactive timeout* – skončil už tok?
  - *active timeout* – včasný sběr dlouhotrvajících toků

Dostupná řešení pro monitorování toků – I



Dostupná řešení pro monitorování toků – II

Směrovače – CISCO, Juniper, Enterasys, ...

- Zaneprázdněny směrováním, monitorování toků jako doplněk.
- Monitorování toků není implementované ve všech modelech.
- Fixní umístění, možný cíl útoků.
- Často nezbytné vzorkování, omezené pokročilé technologie.

Dostupná řešení pro monitorování toků – III

SW NetFlow Sondy – nProbe, yaf, fprobe, softflowd, ...

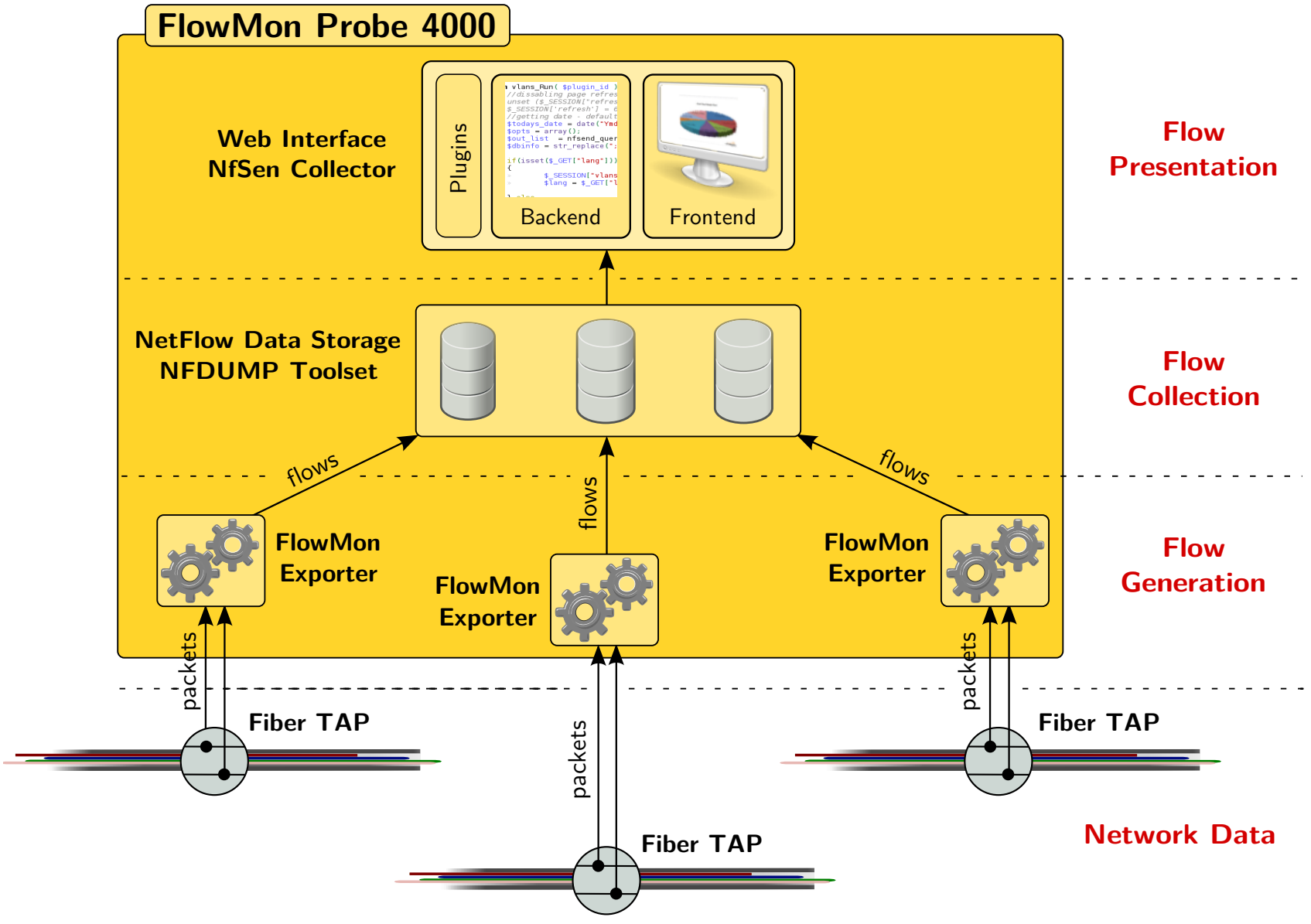
- Založeno na běžném HW – PC a běžných síťových kartách.
- Limitovaný výkon (PCAP, PCI) a problémy stability.
- Vyžaduje expertní úpravy a nastavení měřicího systému.
- Zaplňují mezeru kde potřebujeme monitorovat a není čím.

Hardwarově akcelerované sondy

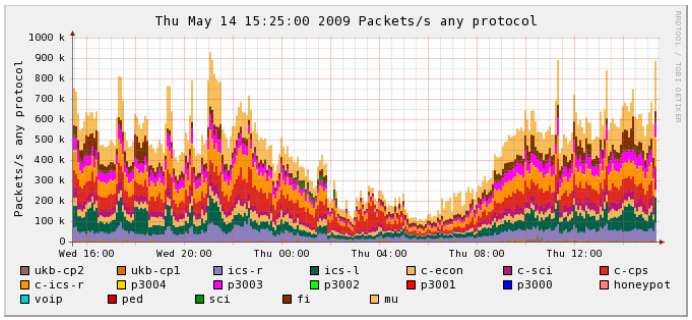
- Sběr statistických informací o tocích je taktéž náročný na použitý hardware ⇒ vznik specializovaných HW sond.
- Kromě vysoké propustnosti je možné pracovat s přesnějším časem (<ns) než v případě SW sond (ms).
- Nevýhoda: vysoká cena.

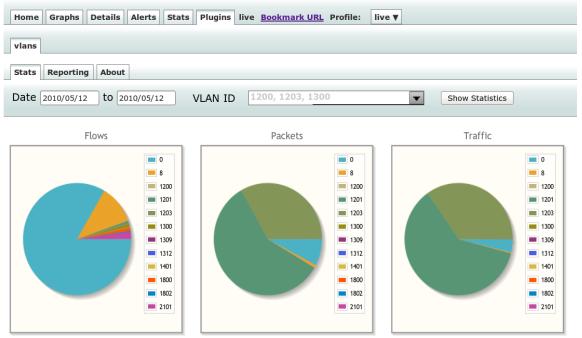
- Základní výzkum proběhl i v rámci aktivity Programovatelný hardware sdružení CESNET ve spolupráci s VUT a MU.
- V projekt EU FP6 GÉANT2 vznikl *GN2 Security Toolset*, který tvoří HW sonda *FlowMon* a kolektor *NfSen*.
- Tato kombinace je dnes nasazena a používána i v síti MU.
- Aktuální výzkum a vývoj: IPFIX, tzv. „extended" NetFlow – rozšíření klasické pětice tvořící klíč toku o další, uživatelem definované položky.

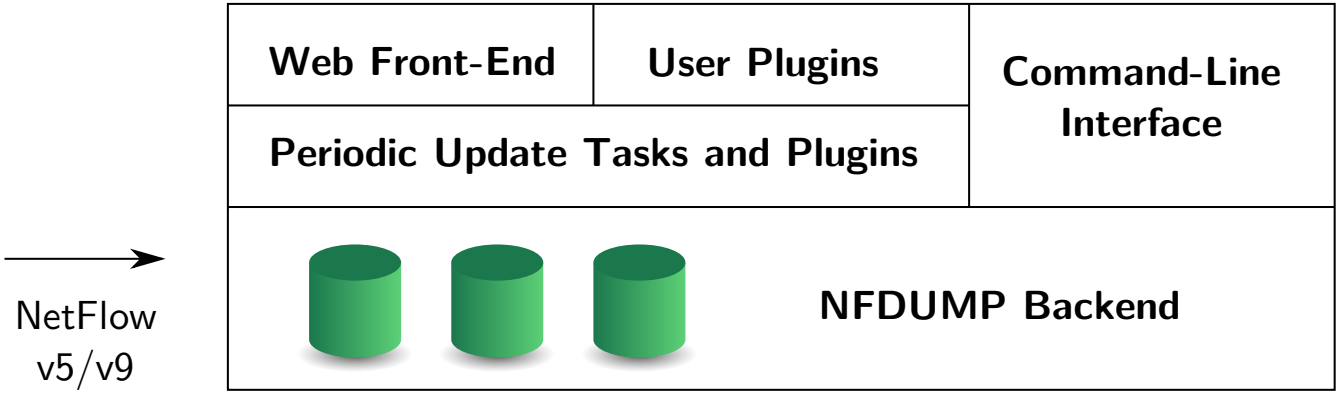
Architektura sondy FlowMon



Architektura kolektoru NfSen/NFDUMP







- **NfSen – NetFlow Sensor** – `http://nfsen.sf.net/`
- **NFDUMP – NetFlow display** – `http://nfdump.sf.net/`

Zpracování NetFlow dat nástrojem NFDUMP

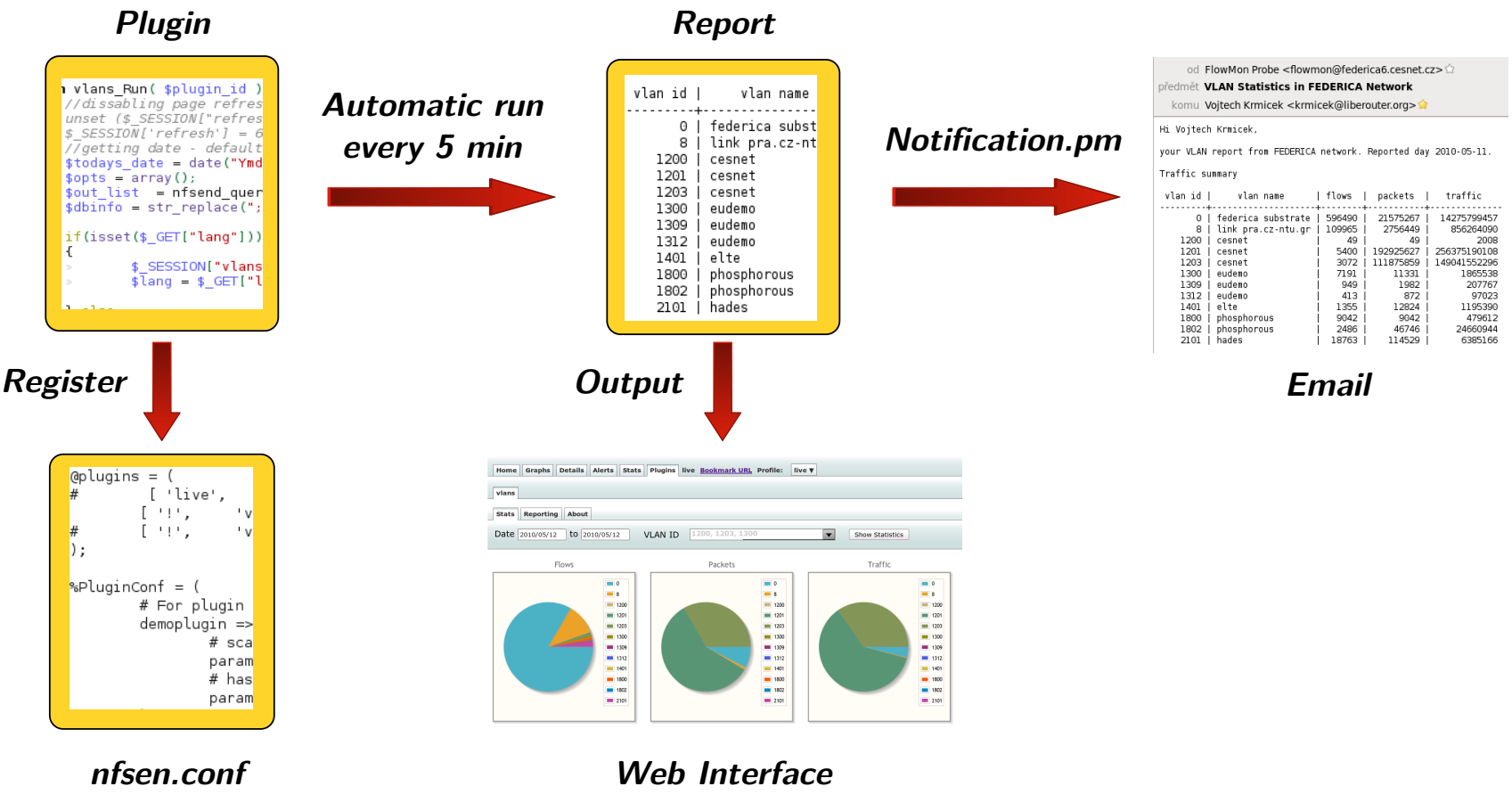
Dostupné flow statistiky

- Výpis NetFlow dat.
- Top N statistiky.
- Filtrování toků (podle IP adres, protokolů, VLAN, MAC, ...).
- Agregování toků (podle IP adres, protokolů, VLAN, ...).

```
Flow start    Duration Proto    Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes  Intf  VLAN
06:49:55.049   299.996 ICMP     192.168.3.2:0    ->     192.168.3.1:0.0        969    1.3 M    8   1203
06:49:55.657   299.997 ICMP     192.168.3.1:0    ->     192.168.3.2:8.0        969    1.3 M    9   1203
06:51:10.255   299.752 ICMP     192.168.3.2:0    ->     192.168.1.1:8.0        968    1.3 M    8   1203
06:51:10.255   299.752 ICMP     192.168.1.1:0    ->     192.168.3.2:0.0        968    1.3 M    9   1203
06:51:36.593   299.824 ICMP     192.168.1.3:0    ->     192.168.1.1:0.0       1936    2.6 M    6   1201
06:51:37.189   299.848 ICMP     192.168.1.1:0    ->     192.168.1.3:8.0       1936    2.6 M    7   1201
06:54:55.355   299.997 ICMP     192.168.3.2:0    ->     192.168.3.1:0.0        969    1.3 M    8   1203
06:54:55.964   299.996 ICMP     192.168.3.1:0    ->     192.168.3.2:8.0        969    1.3 M    9   1203
06:56:10.317   299.781 ICMP     192.168.1.1:0    ->     192.168.3.2:0.0        968    1.3 M    9   1203
06:56:10.317   299.781 ICMP     192.168.3.2:0    ->     192.168.1.1:8.0        968    1.3 M    8   1203
06:56:36.649   299.916 ICMP     192.168.1.3:0    ->     192.168.1.1:0.0       1936    2.6 M    6   1201
06:56:37.245   299.941 ICMP     192.168.1.1:0    ->     192.168.1.3:8.0       1936    2.6 M    7   1201
06:57:01.952     0.000 UDP    194.132.52.193:138 -> 194.132.52.195:138          2      513    5   1200
```

Zásuvné moduly (pluginy) pro NfSen

- Pluginy umožňují rozšíření NfSenu o nové funkce.
- Pluginy jsou automaticky spouštěny každých 5 minut.
- Pluginy umožňují zobrazit výsledky naměřených NetFlow dat.



Další zdroje

- M. Patterson: Where NetFlow and Packet Capture Complement Each Other

  `http://sharkfest.wireshark.org/sharkfest.10/B-3_Patterson%20Where%20NetFlow%20and%20Packet%20Capture%20Complement%20Each%20Other.ppt`
- J. White: Using NetFlow to Analyze Your Network

  `http://sharkfest.wireshark.org/sharkfest.11/presentations/I-7_White-Using_NetFlow_to_Analyze_Your_Network.pdf`
- Skupina analýzy provozu sítě

  `http://www.muni.cz/ics/saps/web/`

Shrnutí

- Pro bezpečnostní aplikace je výhodné trvalé pasivní monitorování.
- Nasazení SNMP či sběr Syslogu vyžaduje konfigurovat dotčené prvky.
- Analýza síťového provozu je pro uživatele transparentní.
- Prohledávání obsahu všech paketů je ve vysokorychlostních sítích nemožné.
- Používá se monitorování síťových toků (typicky na síťové až transportní vrstvě), které poskytuje kýženou agregaci a přitom zachovává informační hodnotu (na rozdíl od SNMP).