FlowMon – Vaše síť pod kontrolou!

kompletní řešení pro monitorování a bezpečnost počítačových sítí

Jiří Tobola
tobola@invea.cz

INVEA-TECH: od aplikovaného ICT výzkumu k podnikatelské příležitosti

invea tech Váš partner ve světě vysokorychlostních sítí

Jak to začalo..

- CESNET založil v roce 2002 projekt Liberouter
- Spolupráce s Masarykovou univerzitou a VUT v Brně
- Cíle:
  - akcelerace vysokorychlostních síťových aplikací (IPv6 router)
  - využití technologie programovatelného hardware
  - vývoj hardwarových akcelerátorů COMBO založených na technologii FPGA pro urychlení kritických úloh při zpracování dat
- Participace na EU projektu 6NET (IST-2001-32063)
- Postupný růst a vybudování silného R&D týmu v oblasti programovatelného hardware a vysokorychlostních síťových aplikací

..pokračovalo..

- Úspěšné zakončení projektu 6NET
- Spolupráce na dalších EU projektech
- SCAMPI (IST-2001-32404)
  - 2002 – 2005, monitorování sítí o rychlostech 10 Gb/s
  - připojení se k projektu v roce 2003 namísto komerčních partnerů
  - vytvoření funkčního prototypu, úspěšná obhajoba
  - doporučení – komercializovat výsledky v praxi
- GEÁNT2 (contract No. 511082)
  - spolupráce 26 NRENs reprezentujících 34 zemí
  - aktivita JRA2 se zaměřením na síťovou bezpečnost
  - vytvoření funkčního prototypu HW akcelerované NetFlow sondy
  - výsledné doporučení – monitorovat sítě pomocí této sondy

..skončilo, resp. začalo:)

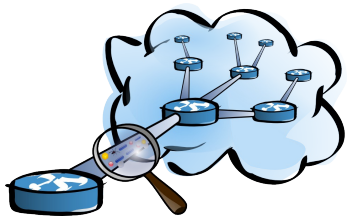
- 6. června 2007 – založení firmy INVEA-TECH a.s.
- Jeden z prvních spin-offů s účastí univerzit
- Zakladatelé:
  - společnost UNIS – technologický partner
  - fyzické osoby
  - Masarykova univerzita
  - Vysoké učení technické v Brně
- Technologický transfer z CESNETu do INVEA-TECH a.s.
  - problém s hledáním vhodného modelu
  - první technologický transfer z CESNETu

Oblasti působení firmy

- Vývoj a prodej bezpečnostních a monitorovacích systémů (nejen) pro vysokorychlostní sítě
- Bezpečnostní analýzy na základě technologie NetFlow
- Využití technologie programovatelného hardware (FPGA) pro akcelerace výpočetně náročných úloh
- Zakázkový vývoj FPGA IP cores
- Vývoj kompletního prostředí pro rychlý vývoj aplikací nad technologií FPGA pro různé hardwarové platformy (ve spolupráci s akademickými partnery)

Portfolio produktů

- Síťová oblast
  - FlowMon – řešení pro monitorování sítí na základě IP toků (NetFlow)
  - Snort Accelerator – hardwarově akcelerované IDS sondy
  - NIFIC – hardwarově akcelerovaný firewall pro 10 GE sítě
  - Bezpečnostní analýzy sítí
- FPGA design
  - NetCOPE – platforma pro rychlý vývoj síťových aplikací
  - COMBO HW – PCI Express akcelerační karty s výkonnými FPGA
  - VHDL IP cores – jednotky pro zpracování síťového provozu, řadiče pamětí, sběrnice pro rozvod po čipu



Působení na trhu

- Složité počátky..
  - akcelerovaná karta vs řešení
  - malé povědomí o komerčním prostředí
  - trh neznal technologii
- ..nicméně
  - počáteční problémy překonány
  - a věříme že budeme vzorem pro spoustu dalších spin-offů v ČR

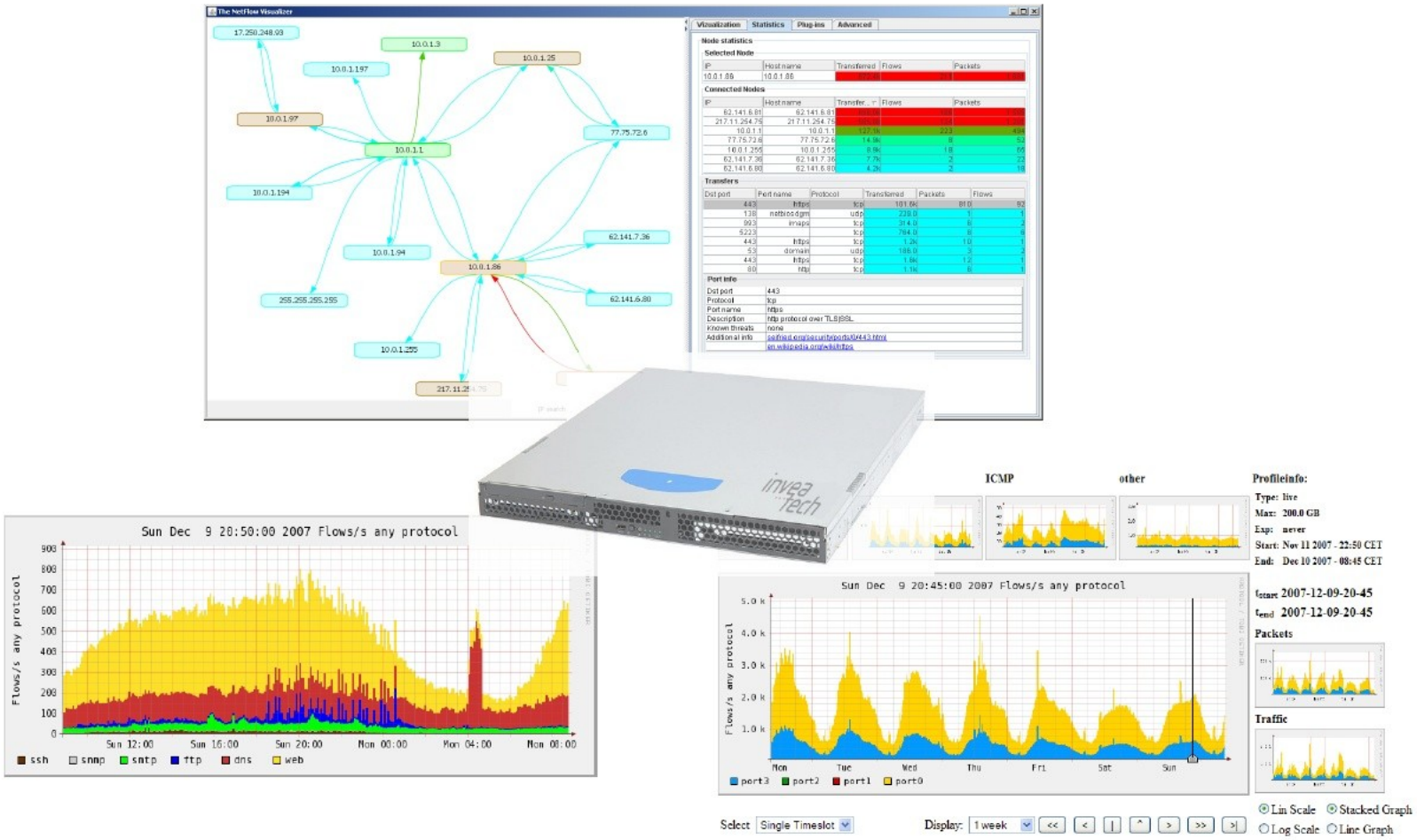
Reference - ČR

- 50 instalací během prvního roku působení na trhu
- Desítky provedených analýz a měření sítí, např.
- Potenciálním zákazníkem je každá organizace spravující 40 a více počítačů v síti
- Zákaznické reference
  - akademická sféra – univerzity, knihovny, AV
  - státní sféra – magistráty, kraje, nemocnice
  - soukromá sféra – od malých až po největší společnosti
  - poskytovatelé internetu

Reference - svět

- Koncoví uživatelé
  - GEÁNT2 – monitoring 7 evropských páteřních sítí
  - IT&TEL Rakousko, Pitcom ISP Německo
- Obchodní partneři
  - Contech - USA
  - CQVista – Jižní Korea
  - 8 evropských zemí
- Technologičtí partneři
  - Group2000 – Holandsko
  - NETi – Maďarsko
  - Comcraft - Francie

FlowMon


Sun Dec 9 20:50:00 2007 Flows/s any protocol
Flows/s any protocol
ssh
snmp
smtp
ftp
dns
web
ICMP
other
Profileinfo:
Type: live
Max: 200.0 GB
Exp: never
Start: Nov 11 2007 - 22:50 CET
End: Dec 10 2007 - 08:45 CET
Sun Dec 9 20:45:00 2007 Flows/s any protocol
Packets
Traffic
port3
port2
port1
port0
Select
Single Timeslot
Display:
1 week
Lin Scale
Stacked Graph
Log Scale
Line Graph

Síť = základ Vašeho IT

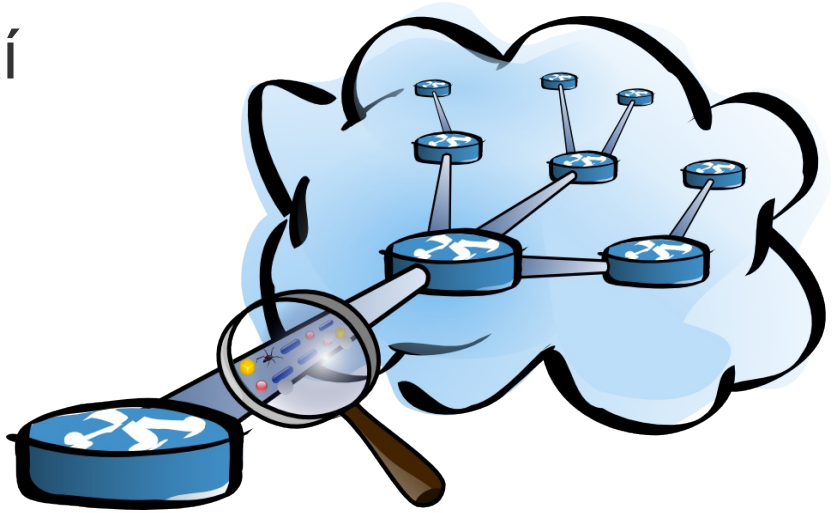
- Víte kolik Vaši organizaci nákladově stojí hodina nefungování sítě?
- Víte jakou hodnotu mají data která jsou dostupná ve Vaši počítačové sítí?
- Máte zajištěnu vnější i vnitřní bezpečnost sítě?
- Na fungování sítě závisí:
  - aplikace
  - dostupnost dat
  - uživatelé
  - zákazníci
  - obchody
  - chod organizace
  - image organizace

Znáte do detailu svou síť?

- Víte o všem co se děje ve Vaší síti?
- Jste si jistí bezpečnostní Vaší sítě?
- Je Vaše síť chráněna proti vnějším i vnitřním útokům?
- Máte možnost sledovat síťový provoz v reálném čase?
- Odhalujete problémy na síti rychle a jednoduše?
- Máte dostatek informací pro optimalizaci a rozšiřování síťové infrastruktury?
- Snadno dohledáváte a prokazujete bezpečnostní incidenty?
- Víte, kteří uživatelé a které služby nejvíce zatěžují Vaši síť?
- Znáte reálné využití Internetu?
- Kontrolujete dodržování peering dohod a SLA?

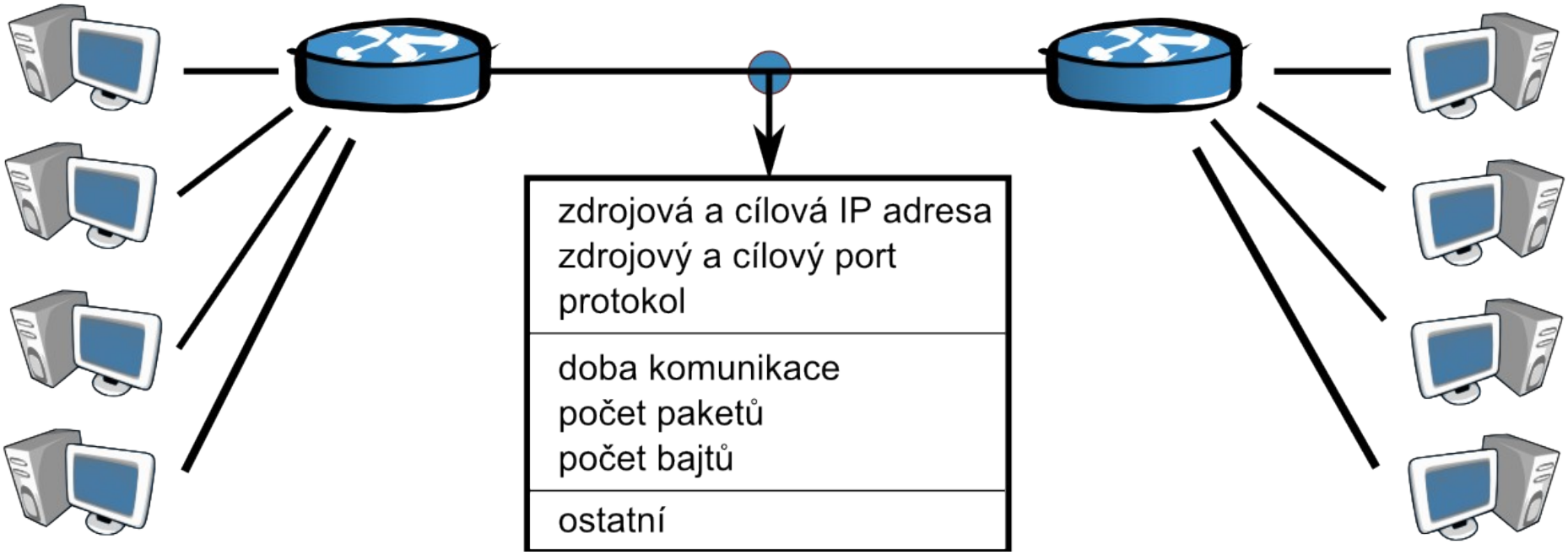
FlowMon – síť pod kontrolou!

- Kompletní řešení pro monitorování sítě na základě IP toků
- Založeno na technologii NetFlow v5/v9
- Poskytuje informace kdo, s kým, jak dlouho, jakým protokolem komunikoval a kolik přenesl dat
- Odpověď na všechny otázky z předcházejícího slajdu
- Nejlepší poměr cena/výkon na trhu
- Unikátní přínos pro uživatele
- Řešení pro sítě všech velikostí
- Technologie vytvořená v ČR



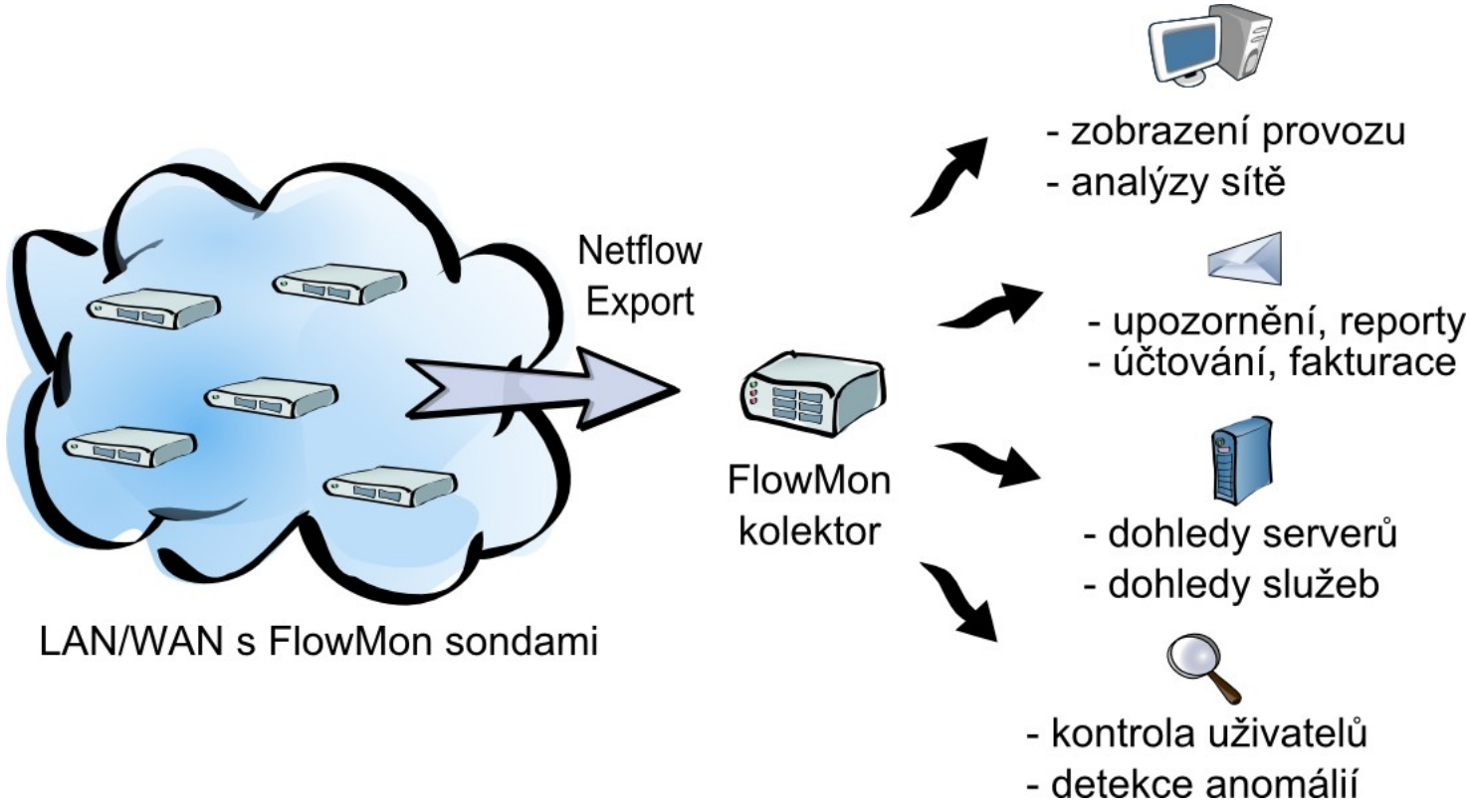
Technologie NetFlow

- Měření na základě IP toků
- Moderní metoda monitorování sítí
- Cisco standard v5/v9
- Redukce dat cca 500:1

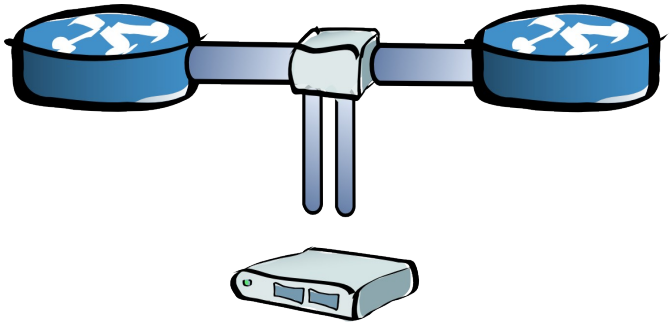


FlowMon architektura

- Pasivní FlowMon sondy
  - zdroj síťových statistik (NetFlow dat)
- Kolektory NetFlow dat
  - vizualizace a vyhodnocení síťových statistik

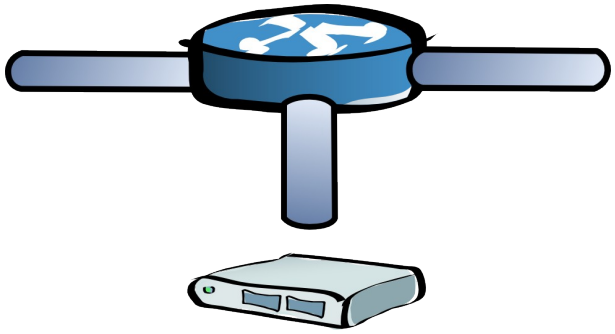


Zapojení FlowMon sond v síti



Metalický/optický rozbočovač

- TAP mode
- páteřní linky
- připojení k internetu

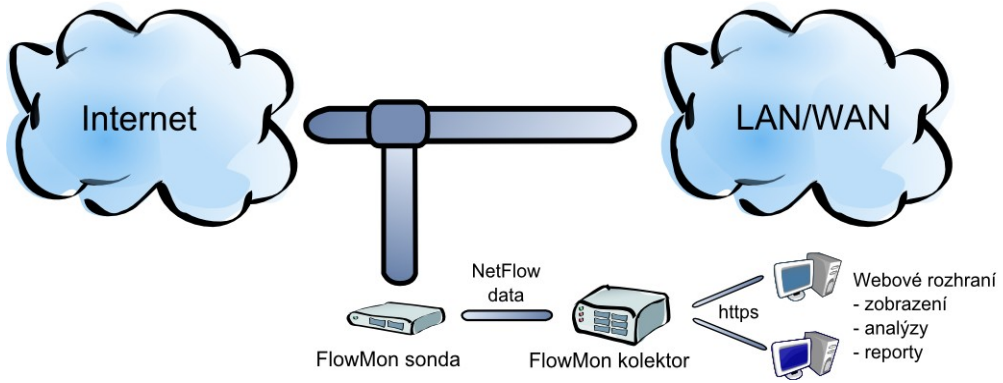


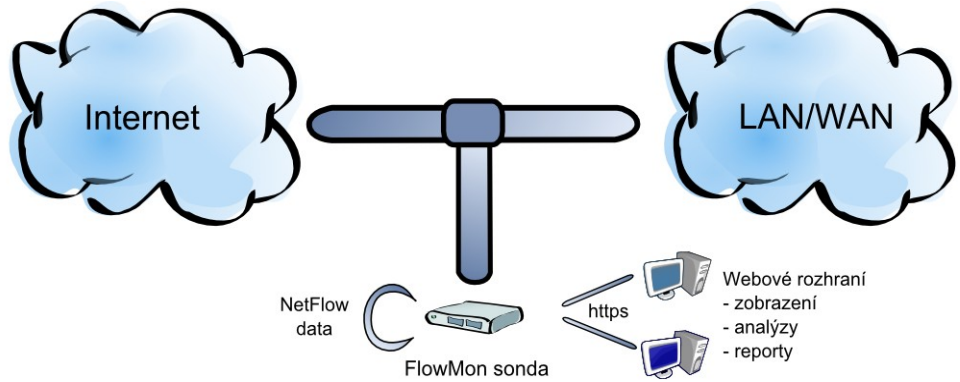
Mirror port aktivního prvku

- SPAN mode
- monitoring LAN

FlowMon sondy

- Výkonné autonomní NetFlow sondy - zdroj záznamů o IP tocích ve formátu NetFlow v5/v9/IPFIX
- Mobilní, L2/L3 neviditelná zařízení – transparentní pro monitorovanou síť, použitelná v libovolném bodě sítě
- Standardní a hardwarově akcelerované modely
- Vzdálená konfigurace přes intuitivní webové rozhraní
- Podpora 10/100/1000 Ethernetu, 10 GE, IPv4, IPv6, VLAN
- Vestavěný kolektor pro okamžité uložení a analýzu dat





Standardní modely

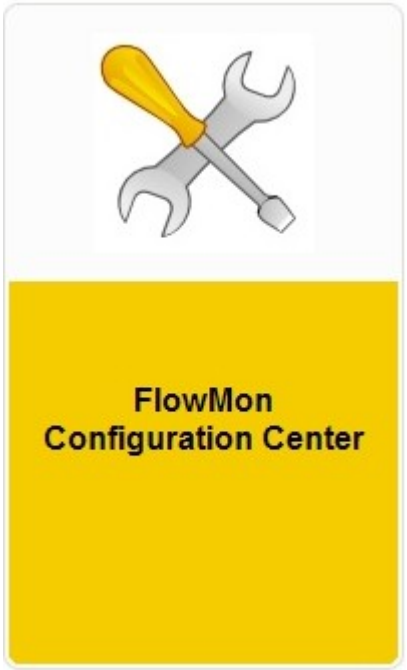
- Kompaktní 1U sondy s dobrým výkonem za nízkou cenu
- Vhodné pro menší a střední sítě (výkon více než 500 000 paketů za vteřinu)
- Metalická i optická rozhraní, modely se SFP a SFP+ porty
- Modely FlowMon Probe 1000/2000/4000/6000/10000/20000
- Jeden administrativní a až 6 monitorovacích 10/100/1000 Ethernet portů nebo až dva 10 GE monitorovací porty

Akcelerované modely

- Využití technologie programovatelného hardware
- Maximální výkon a stabilita
- Neunikne žádný paket, zpracování na rychlosti linky
- 15 miliónů paketů za vteřinu na 10GE lince
- Vhodné pro velké sítě a páteřní linky
- Modely FlowMon Probe 4000 Pro, 20000 Pro
- 4 monitorovaná 10/100/1000 Ethernet rozhraní či
  2 desetigigabitové monitorované rozhraní

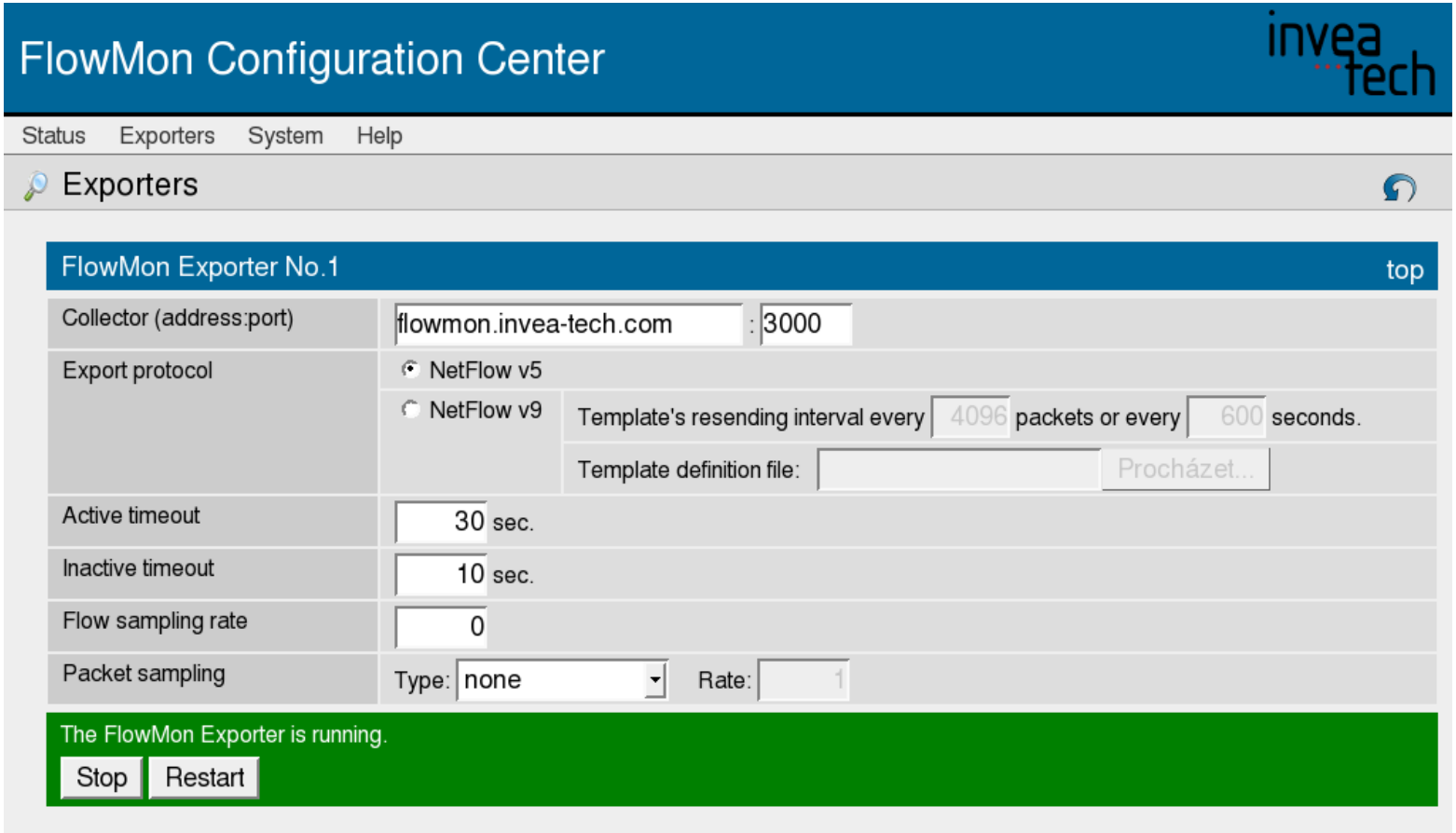
Webové rozhraní sondy

- Intuitivní webové rozhraní se zabezpečeným přístupem
- Nastavení parametrů sondy - FlowMon Configuration Center
- Vizualizace síťových statistik na vestavěném kolektoru – FlowMon Monitoring Center
- Komunikace se sondou přes administrativní síťový port



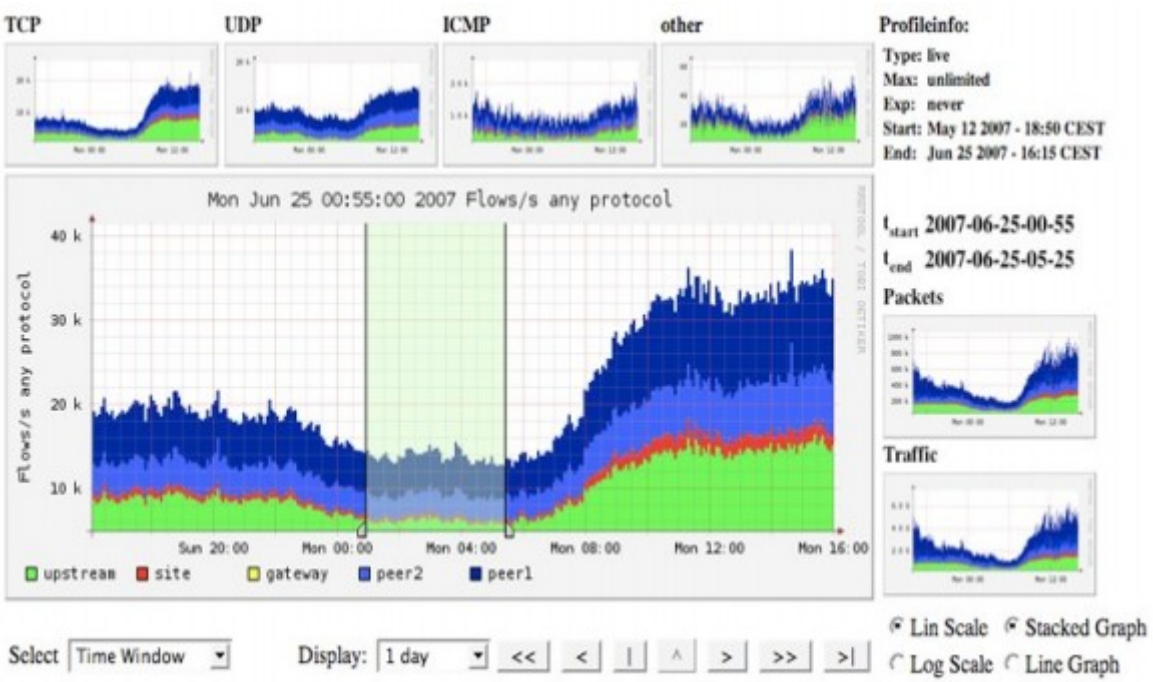
FlowMon konfigurační centrum

- Konfigurace a správa parametrů sondy
- Nastavení cíle exportů, správa uživatelů a další



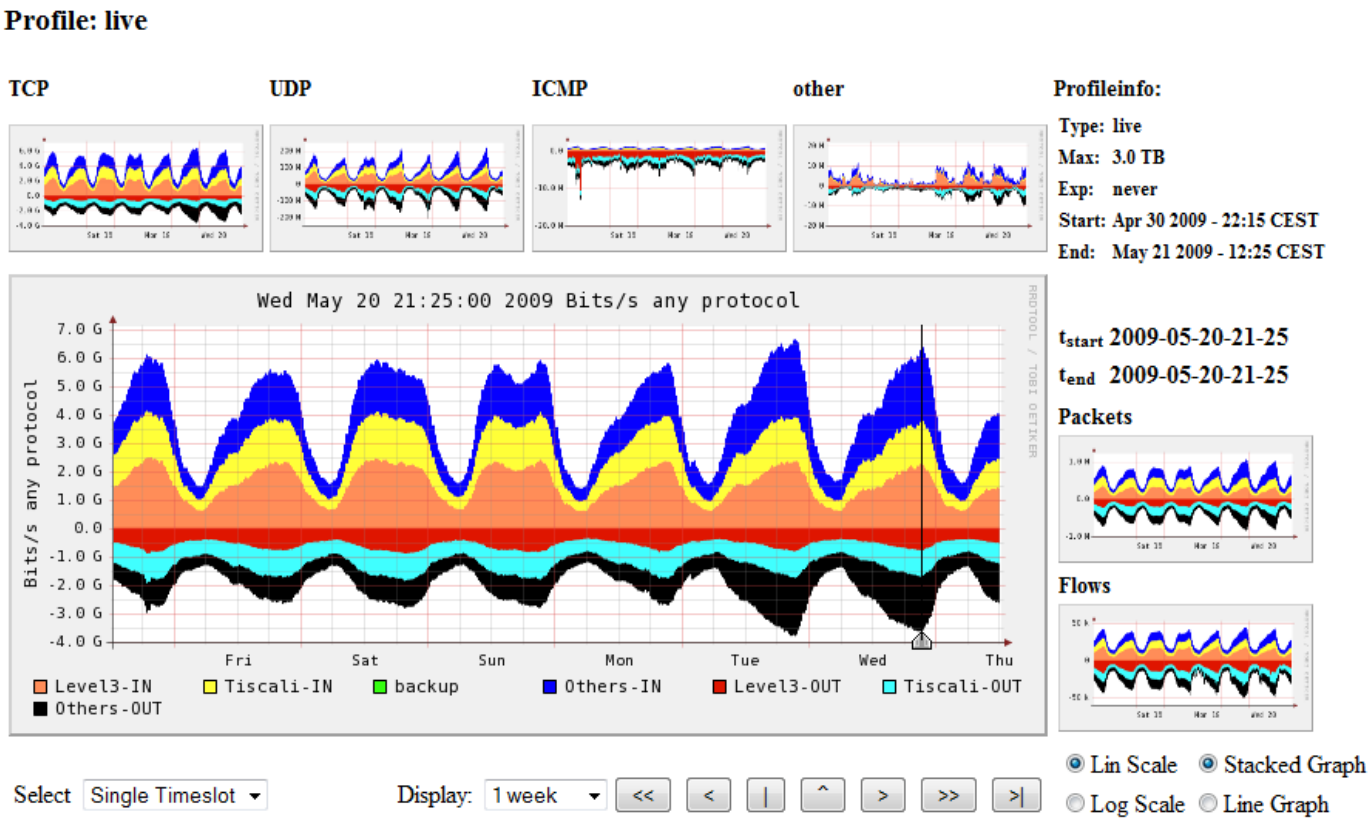
FlowMon monitorovací centrum

- Integrovaný kolektor pro ukládání a vizualizaci statistik
- Grafy a tabulky komunikací, formulář pro detailní analýzy
- Top N statistiky (uživatelé, služby, navštěvované servery)
- Předdefinovaná sada pohledů na standardní protokoly
- Uživatelsky definované pohledy (pobočky, servery, uživatelé)



FlowMon monitorovací centrum

- Dlouhodobý detailní záznam o provozu na síti
- Podpora profilů a upozornění na email (alerty)
- Dohledání libovolné komunikace v síti



FlowMon kolektor

- Dlouhodobé uložení NetFlow statistik z několika zdrojů
- Zařízení s možností volby aplikace pro vizualizaci statistik
  - FlowMon monitorovací centrum – vždy v ceně zařízení
  - Caligare Flow Inspector
  - NetFlow Tracker
- Zobrazení a analýzy síťového provozu
- Stejné rozhraní jako u vestavěného kolektoru na sondě
- Profesionální řešení pro větší sítě
  - RAID, redundantní napájení, úložná kapacita 1 TB – 100 TB
  - dohled nad sítí z centrálního bodu v síti

FlowMon rozšiřující moduly

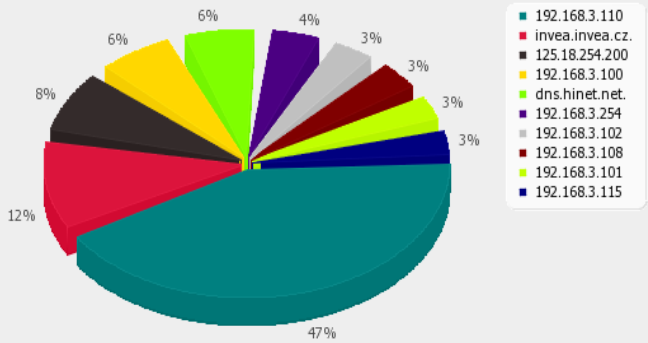
- Rozšiřující aplikační moduly
- Integrace do webového rozhraní sondy/kolektoru
  - dohledové nástroje (MRTG, Zabbix, Nagios)
  - FlowMon Reporter – inteligentní reportovací nástroj
  - detekce anomálií a infikovaných počítačů
  - logování navštívených URL, detekce NAT a další
- NFVis - inovační technologie vizualizace NetFlow dat

FlowMon Reporter

- Koláčové grafy nejen pro manažery, export do pdf, csv
- Přehled o tom co se dělo v síti za poslední den/týden/měsíc
- Statistiky online i offline v zadaném intervalu do emailu

Stanice s největším množstvím toků - 16.03.2009(00:00) - 16.03.2009(14:55) top

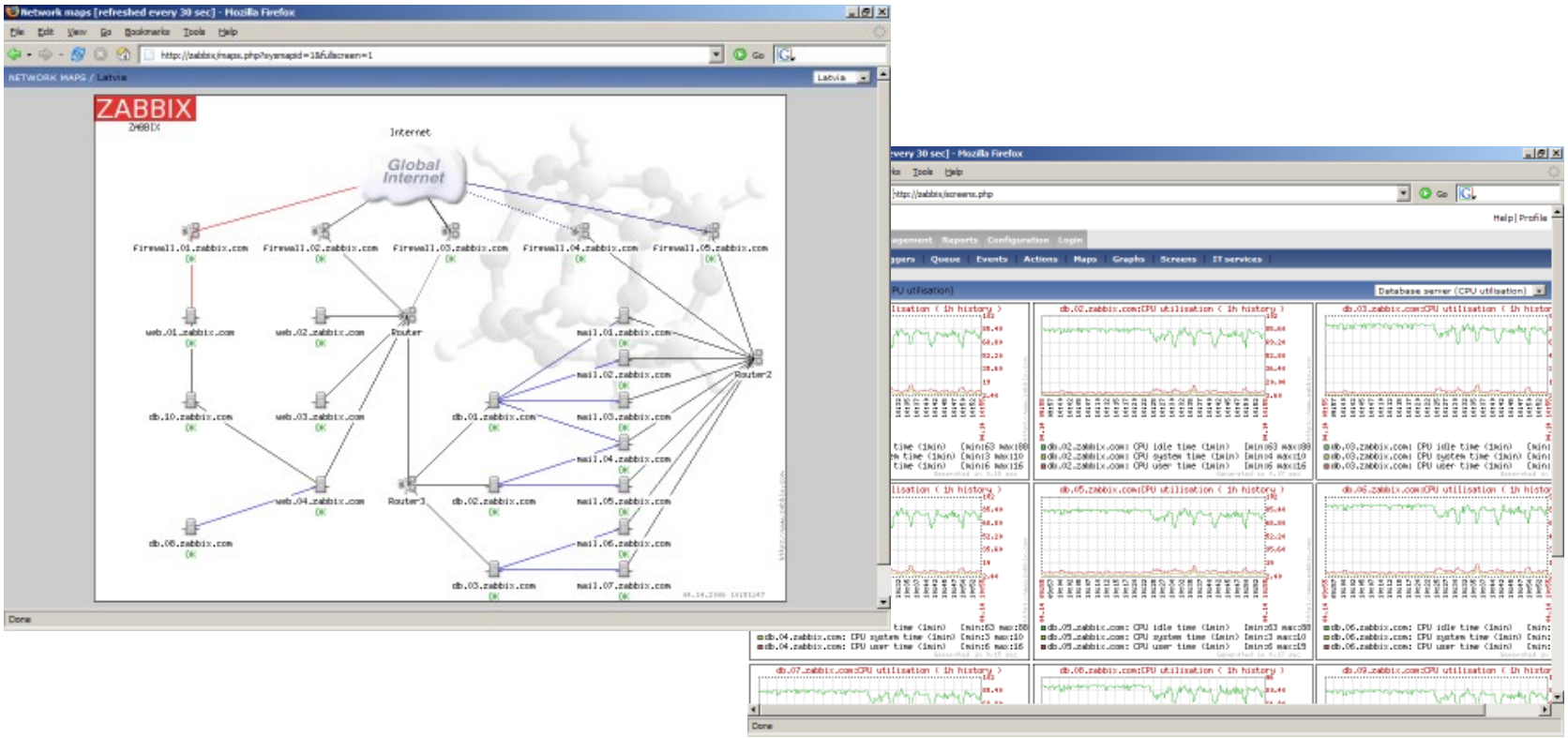
Tato kapitola shrnuje stanice s největším počtem toků zaznamenaných ve sledované síti. Nadměrný výskyt toků může indikovat pokus o prolomení do počítačové sítě (lámání hesel, skenování sítě, aj.) či šíření virů a červů v síti.



	Doménové jméno	IP adresa	Pakety/s	Toky
1.	192.168.3.110	192.168.3.110	10	129.7 k
2.	invea.invea.cz.	212.96.160.170	782	32.89 k
3.	125.18.254.200	125.18.254.200	7	23.33 k
4.	192.168.3.100	192.168.3.100	5	18.96 k
5.	dns.hinet.net.	168.95.1.1	0	17.58 k
6.	192.168.3.254	192.168.3.254	1	11.92 k
7.	192.168.3.102	192.168.3.102	0	10.58 k
8.	192.168.3.108	192.168.3.108	781	10.18 k
9.	192.168.3.101	192.168.3.101	0	9.71 k
10.	192.168.3.115	192.168.3.115	0	9.08 k
	Celkem		**793**	**158.02 k**

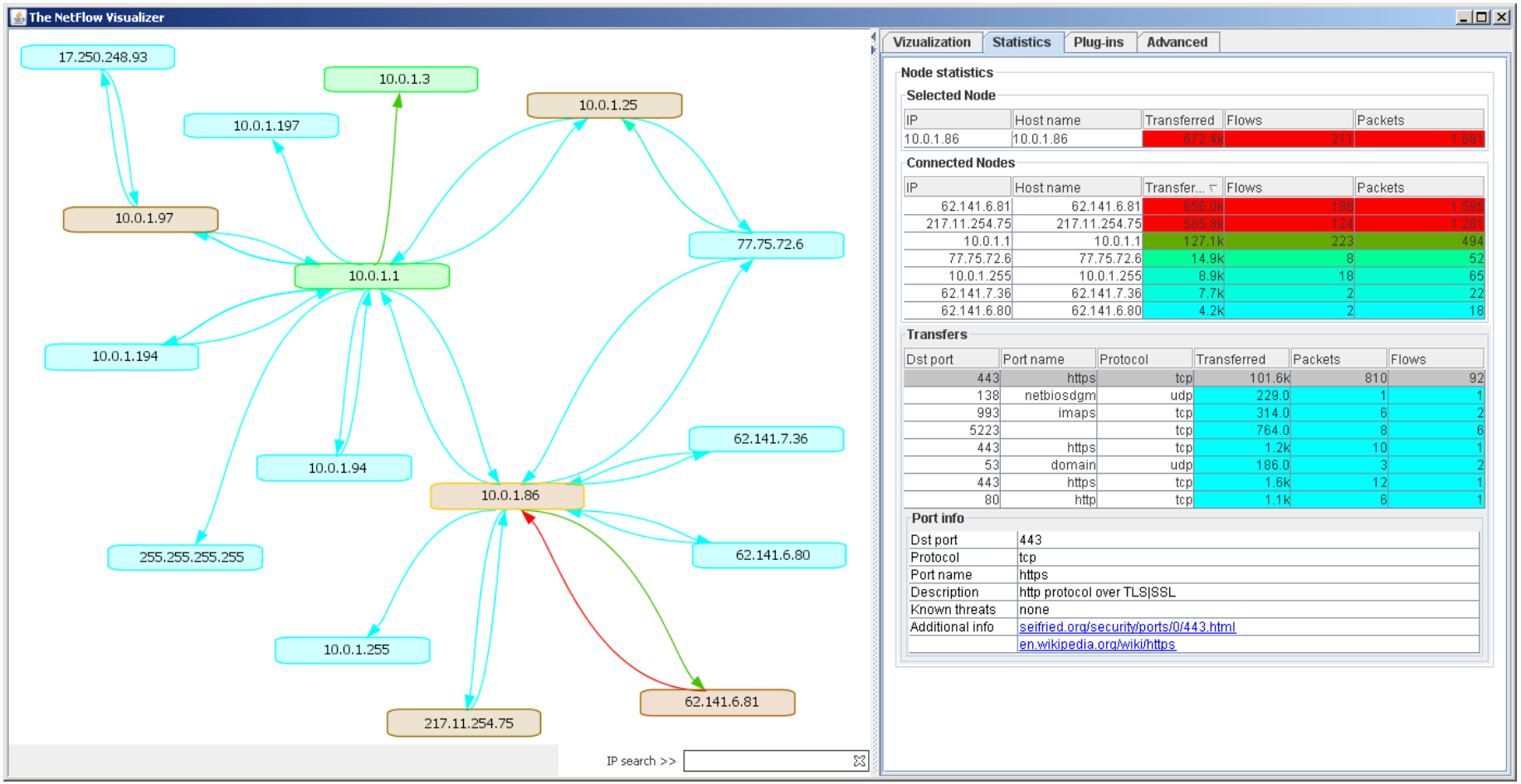
Dohledové nástroje

- Dohled nad prvky sítě a síťovými službami
- Základem je tradiční SNMP monitoring
- Podpora systémů Zabbix/Nagios/MRTG



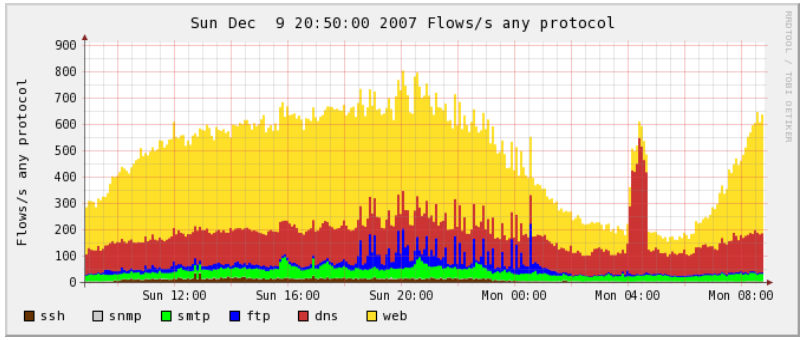
NFVis

- Jediný plugin běžící jako aplikace na uživatelské stanici
- Přehledné zobrazení sítě a objemů přenášených dat



Přínosy pro administrátory..

- Detailní přehled o dění v síti (LAN i WAN) – jak v reálném čase, tak kdykoliv v minulosti
- Přesné, rychlé a efektivní řešení problémů
- Zvýšení bezpečnosti, odhalení vnitřních i vnějších útoků
- Snadné plánování kapacit a optimalizací sítě
- Dohled nad využitím Internetu, využitím aplikací
- Předcházení incidentům jako jsou zahlcení a výpadky sítě
- Odhalení špatných konfigurací



..bezpečnost a management..

- Přínosy řešení pro bezpečnostní oddělení:
  - kontrola přístupů uživatelů k datovým zdrojům
  - dohledávání a prokazování bezpečnostních incidentů
  - porovnání bezpečnostních politik se skutečným stavem v síti
  - prevence před únikem informací ze společnosti
- Přínosy řešení pro management:
  - snížení nákladů na správu a provoz sítě
  - statistiky (tabulky, koláčové grafy) o využití sítě
  - kontrola využívání elektronických zdrojů zaměstnanci (např. využití Internetu v pracovní době)
  - omezení využívání p2p aplikací ap.

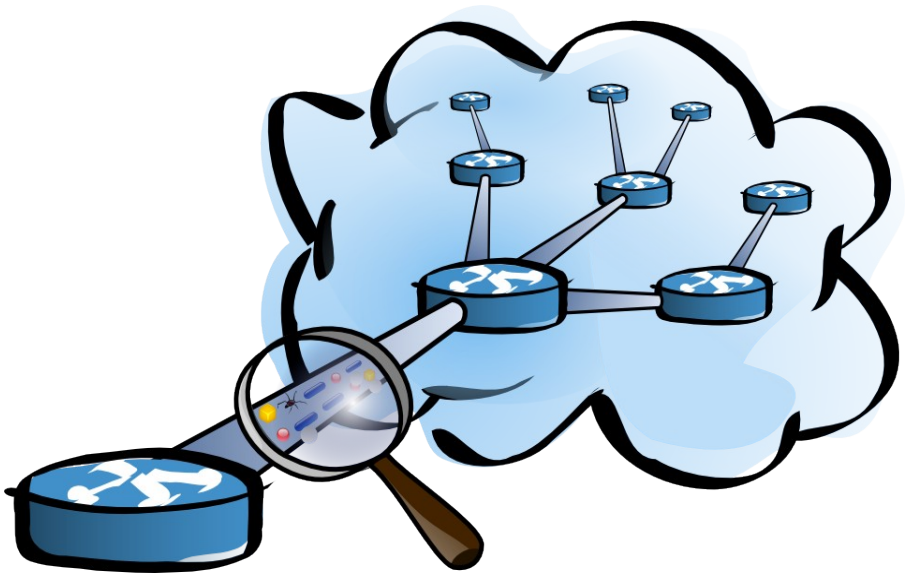
..poskytovatele internetu (ISP)

- Dlouhodobé uložení informací o přenesených datech
- Plánování síťových kapacit na základě trendů
- Optimalizace nákupu konektivity
- Optimalizace peering dohod
- Snadná kontrola a prokazování SLA
- Snadné splnění zákonných požadavků (485/2005)
- Účtování a fakturace na základě přenesených dat
- Možnost integrace grafů a tabulek do vlastního IS

Výhody řešení FlowMon

- Úplná řada produktů pro monitorování všech typů sítí
- Škálovatelnost a flexibilita řešení
- Nejlepší poměr cena/výkon
  - cenová dostupnost standardních modelů
  - vysoký výkon akcelerovaných modelů
- Unikátní přínos pro uživatele

- Nenabízíme ale pouze řešení pro provoz a praxi ale i velmi zajímavou příležitost pro vědu a výzkum!



FlowMon - případové studie

- Monitorování a správa sítě
- Bezpečnost sítě a detekce anomálií
- Rychlé a efektivní dohledávání problémů (troubleshooting)
- Plánování sítě a kapacity linek
- Účtování a fakturace
- Dodržování vyhlášky č. 485/2005

Sledování a správa sítě

- Detailní statistika a ukládání všech aktivit na síti
- Dohledání každé komunikace na síti
- Identifikace TOP uživatelů, služeb, navštěvovaných serverů
- Monitorování síťového provozu v reálném čase i dlouhodobě
- Monitoring LAN, WAN a Internetu
- Kontrola využití Internetu (video, p2p..)
- Dohled serverů a služeb
  - upozornění na problém dříve než si stěžuje vedení / uživatelé / zákazníci
  - šetření nákladů na správu IT infrastruktury

Bezpečnost a detekce anomálií

- Detekce DOS/DDOS, SYN SCAN a dalších útoků
- Odhalení vnějších i vnitřních hrozeb
  - perimetr je většinou dobře zabezpečen
  - zdrojem problémů bývá často lokální síť a vlastní uživatelé
- Často je vhodné proměřit, zkontrolovat zda firewall / UTM dělají to co mají
- Spolehlivé prokazování bezpečnostních incidentů
- Síťové statistiky a behaviorální analýza jsou jedinou šancí jak detekovat ukradené identity a podobné hrozby

Troubleshooting

- Rychlá, efektivní a přesná lokalizace problémů
- Prevence před zahlcením a kolapsem sítě
- Příklady detekovaných problémů
  - nesprávné konfigurace
  - jednoduché odhalení zdrojů problémů
  - vysoký nárůst počtu komunikaci či přenesených dat
  - určení kritických míst sítě
- Podpora upozornění na email / SMS

Plánování sítě a kapacity linek

- SNMP čítače neposkytují dostatečně detailní informace o charakteru provozu
- FlowMon ukazuje přesné složení IP provozu a umožňuje:
  - identifikaci slabých míst v síti
  - určování trendů vývoje a požadavků jednotlivých služeb v čase
  - optimalizovat síť a předejít zbytečným a nákladným upgradům
  - kontrolovat SLA, nákupy konektivity (Internet, pobočky)
  - plánovat a sledovat QoS
- a více nejen pro ISP:
  - optimalizace peering dohod
  - load balancing, router balancing

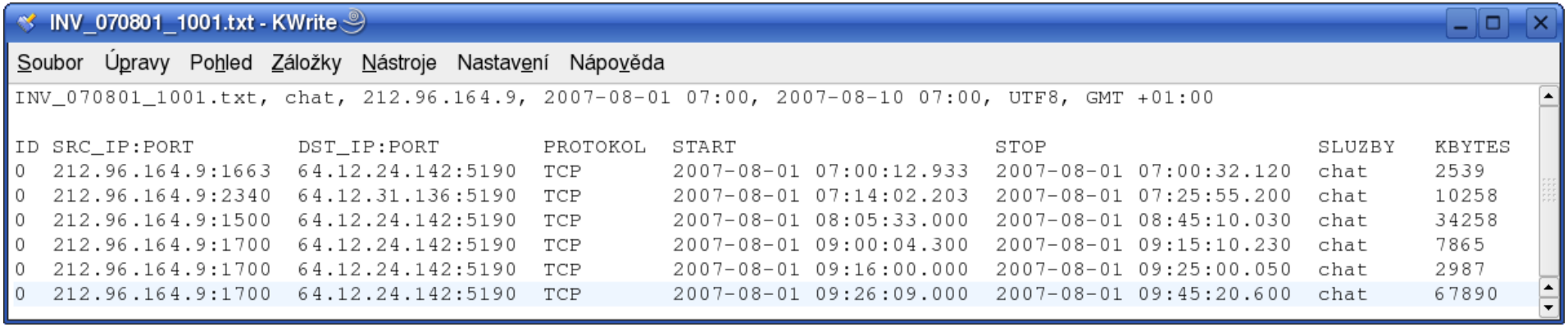
- Cílem je minimalizace celkové ceny síťových operací při maximalizaci výkonu sítě, kapacity a dostupnosti

Účtování a fakturace

- Měření IP provozu a účtování na základě přenesených dat
- 95 percentil a další statistiky potřebné pro účtování
- Automatický zdroj pro fakturaci pro:
  - zákazníky
  - sub-providery
  - oddělení
  - pobočky
- Možnost integrace do IS organizace

Dodržování vyhlášky č. 485/2005

- EU - zákon o sledování elektronické komunikace
- ČR - vyhláška č. 485/2005 ze 7. prosince 2005
- Provozovatelé veřejných komunikačních sítí jsou povinni uchovávat několik měsíců údaje o elektronické komunikaci
- FlowMon řeší bod 3.3.5 vyhlášky - další služby elektronických komunikací
- Strukturovaný výpis datové komunikace - kdo s kým komunikoval a kolik přenesl dat


INV_070801_1001.txt - KWrite

Soubor Úpravy Pohled Záložky Nástroje Nastavení Nápověda

```
INV_070801_1001.txt, chat, 212.96.164.9, 2007-08-01 07:00, 2007-08-10 07:00, UTF8, GMT +01:00

ID SRC_IP:PORT         DST_IP:PORT         PROTOKOL  START                   STOP                    SLUZBY   KBYTES
0  212.96.164.9:1663   64.12.24.142:5190   TCP       2007-08-01 07:00:12.933 2007-08-01 07:00:32.120 chat     2539
0  212.96.164.9:2340   64.12.31.136:5190   TCP       2007-08-01 07:14:02.203 2007-08-01 07:25:55.200 chat     10258
0  212.96.164.9:1500   64.12.24.142:5190   TCP       2007-08-01 08:05:33.000 2007-08-01 08:45:10.030 chat     34258
0  212.96.164.9:1700   64.12.24.142:5190   TCP       2007-08-01 09:00:04.300 2007-08-01 09:15:10.230 chat     7865
0  212.96.164.9:1700   64.12.24.142:5190   TCP       2007-08-01 09:16:00.000 2007-08-01 09:25:00.050 chat     2987
0  212.96.164.9:1700   64.12.24.142:5190   TCP       2007-08-01 09:26:09.000 2007-08-01 09:45:20.600 chat     67890
```

Bezpečnostní analýzy sítí

- Detailní analýzy Vaší sítě se zaměřením na bezpečnost, výkonnost a optimální využití její kapacity
- Nejmodernější metody pro monitorování IP toků
- Nezávislé monitorovací sondy FlowMon
- Bohaté zkušenosti v oblasti sledování a zabezpečení sítí
- Přínosy bezpečnostních analýz:
  - detailní znalost provozu na síti
  - prevence potencionálních bezpečnostních problémů
  - odhalení nesprávných konfigurací
  - rychlé řešení problémů
  - určení kritických míst sítě
  - detailní statistiky aktivit uživatelů a služeb
  - návrh řešení monitorování sítě na bázi NetFlow

Kontaktní informace

Jiří Tobola

tobola@invea.cz

602 647 684

INVEA-TECH a.s.

U Vodárny 2965/2

616 00 Brno

www.invea.cz

Váš partner ve světě vysokorychlostních sítí