



FlowMon – Vaše síť pod kontrolou!

kompletní řešení pro monitorování a bezpečnost počítačových sítí

Jiří Tobola

tobola@invea.cz

invea
tech

Váš partner ve světě vysokorychlostních sítí

- Česká společnost, univerzitní spin-off, spolupráce CESNET a univerzity, projekty EU
- 50 instalací během prvního roku působení na trhu
- Desítky provedených analýz a měření sítí, např.
- Zákaznické reference
 - akademická sféra – univerzity, knihovny, AV
 - státní sféra – magistráty, kraje, nemocnice
 - soukromá sféra – od malých až po největší společnost
 - poskytovatelé internetu
- Mnoho referencí i ze zahraničí, např. Korea Telecom

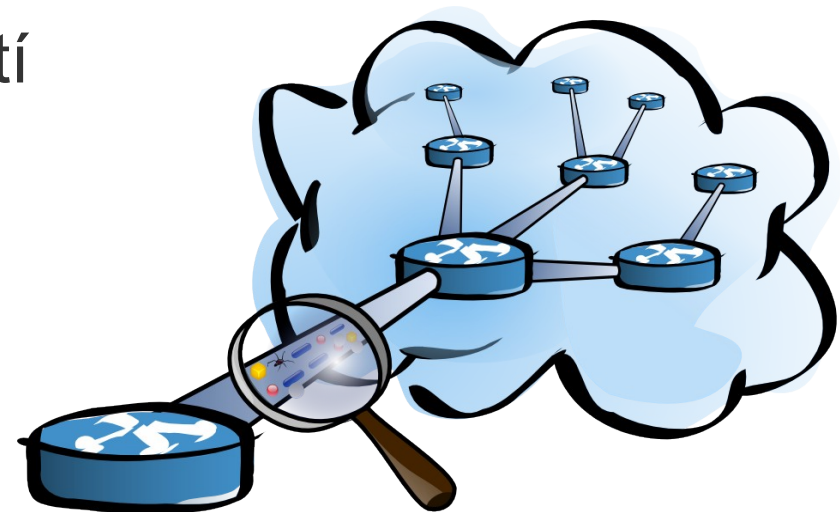


- Víte kolik Vaši organizaci nákladově stojí hodina nefungování sítě?
- Víte jakou hodnotu mají data která jsou dostupná ve Vaši počítačové síti?
- Máte zajištěnu vnější i vnitřní bezpečnost sítě?
- Na fungování sítě závisí:
 - aplikace
 - dostupnost dat
 - uživatelé
 - zákazníci
 - obchody
 - chod organizace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

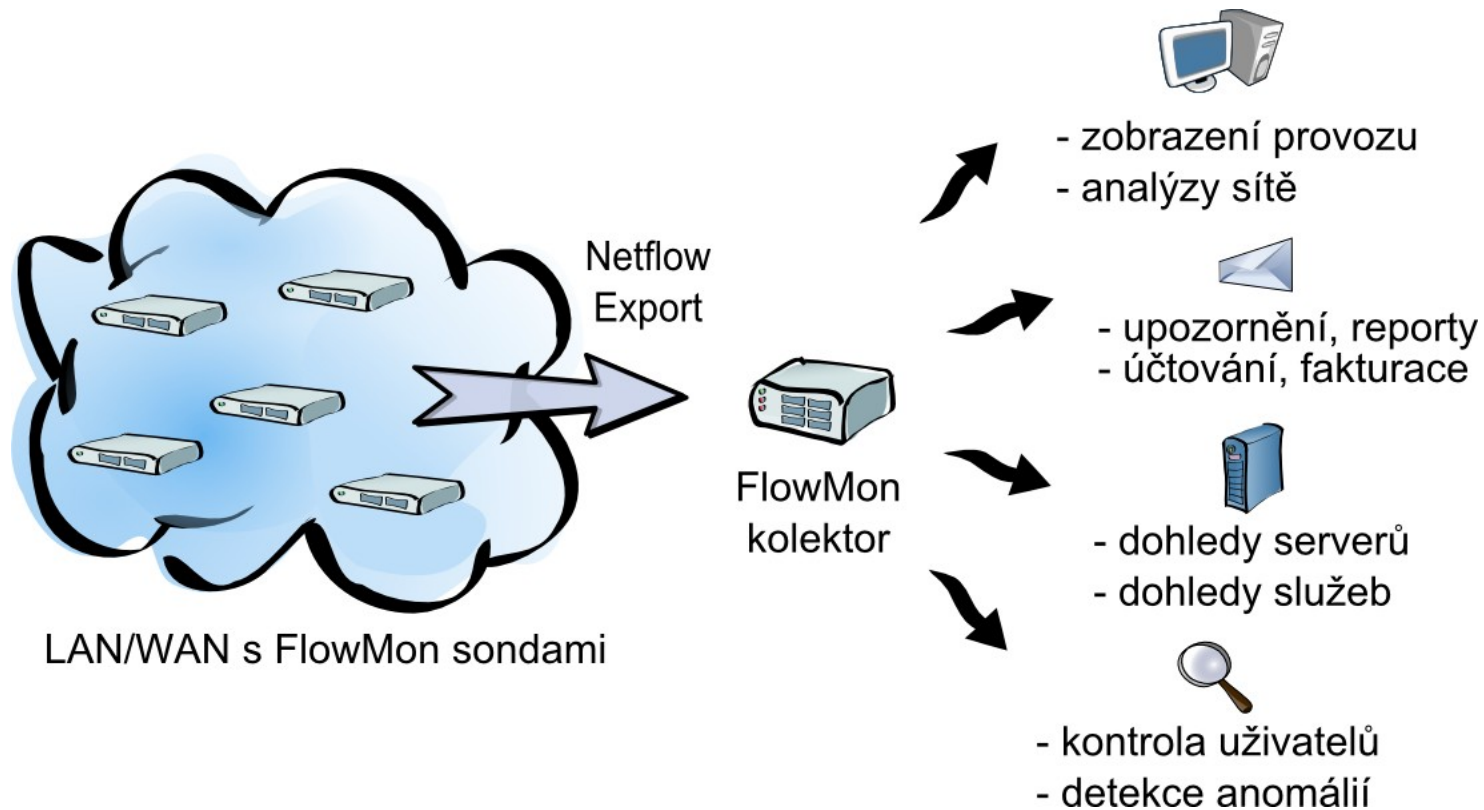


- Víte o všem co se děje ve Vaší síti?
- Jste si jistí bezpečností Vaší sítě?
- Je Vaše síť chráněna proti vnějším i vnitřním útokům?
- Máte možnost sledovat síťový provoz v reálném čase?
- Odhalujete problémy na síti rychle a jednoduše?
- Máte dostatek informací pro optimalizaci a rozšiřování síťové 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?

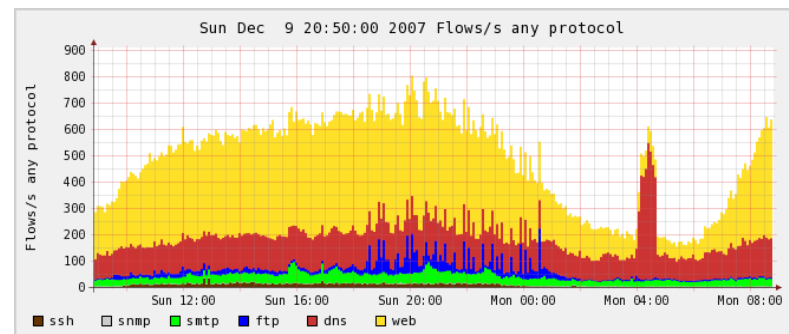
- Kompletní řešení pro monitorování sítě na základě IP toků
- Založeno na technologii NetFlow v5/v9
- Poskytuje informace kdo, s kým, jak dlouho, jakým protokolem komunikoval a kolik přenesl dat
- Odpověď na všechny otázky z předcházejícího slajdu
- Nejlepší poměr cena/výkon na trhu
- Unikátní přínos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



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



- 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



- 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.



- 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



FlowMon - pluginy



FlowMon
Configuration Center



FlowMon
Monitoring Center



Caligare
Flow Inspector



NetFlow Tracker



FlowMon Reporter



FlowMon
Firewall Auditor



FlowMon HTTP Logger



FlowMon Data Retention
485/2005



Nagios



Zabbix



Temperature and
Environmental Monitoring



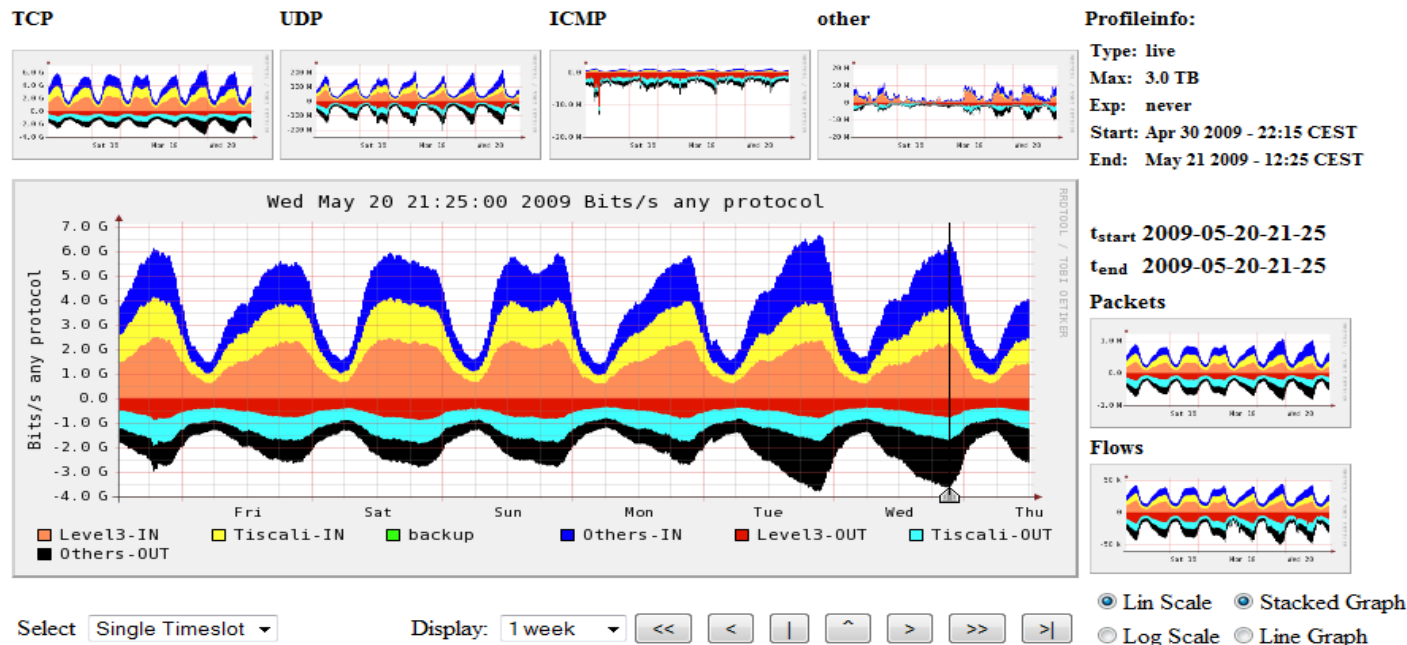
NAT Detective
Will be available soon.

- Aplikace pro uložení a vizualizaci statistik
 - FlowMon monitorovací centrum – vždy v ceně zařízení
 - Caligare Flow Inspector
 - NetFlow Tracker
- Rozšiřující aplikační pluginy
 - FlowMon Reporter
 - FlowMon Firewall Auditor
 - FlowMon HTTP Logger
 - FlowMon Data Retention 485/2005
 - FlowMon NAT Detective
 - FlowMon ADS
 - dohledové nástroje: Zabbix, Nagios
 - samostatné aplikace: NfVis, NfVis Plus

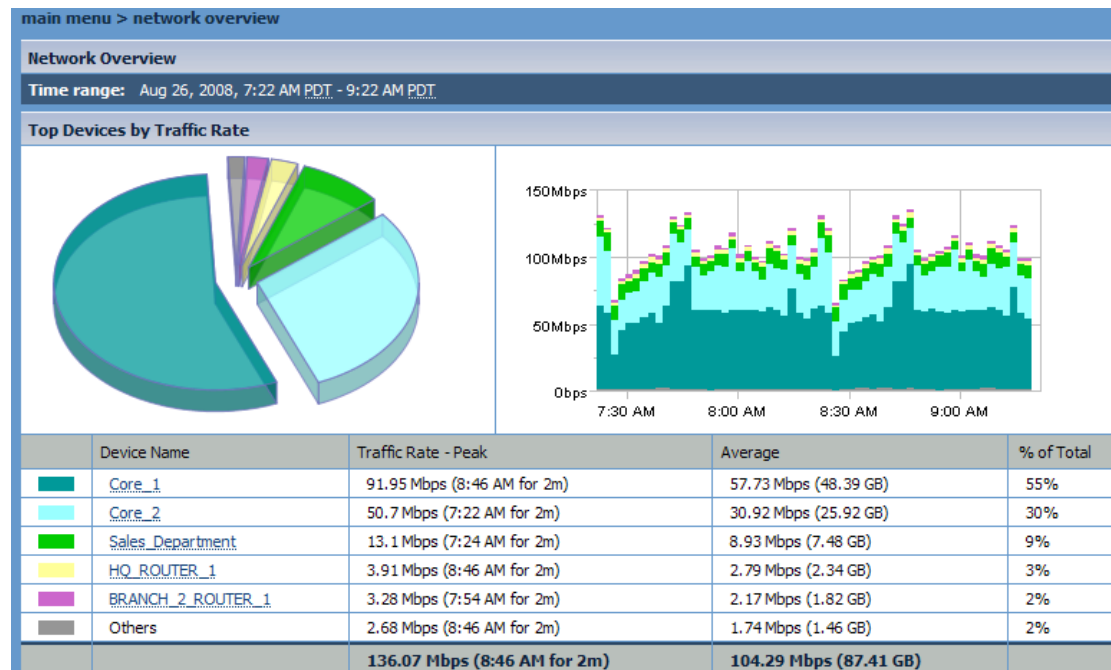
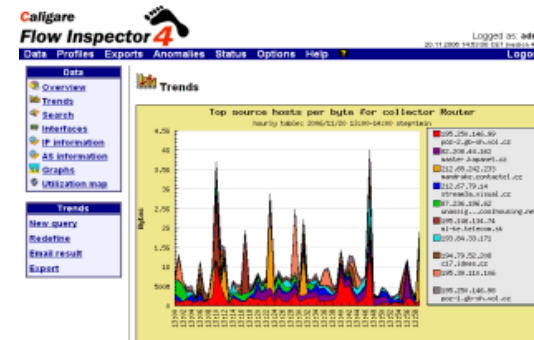


- Grafy a tabulky komunikací, formulář pro detailní analýzy
- Top N statistiky (uživatelé, služby, navštěvované servery)
- Předdefinovaná sada pohledů na standardní protokoly
- Uživatelsky definované pohledy (pobočky, servery, uživatelé)
- Upozornění na email - alerty, dynamické tresholdy

Profile: live

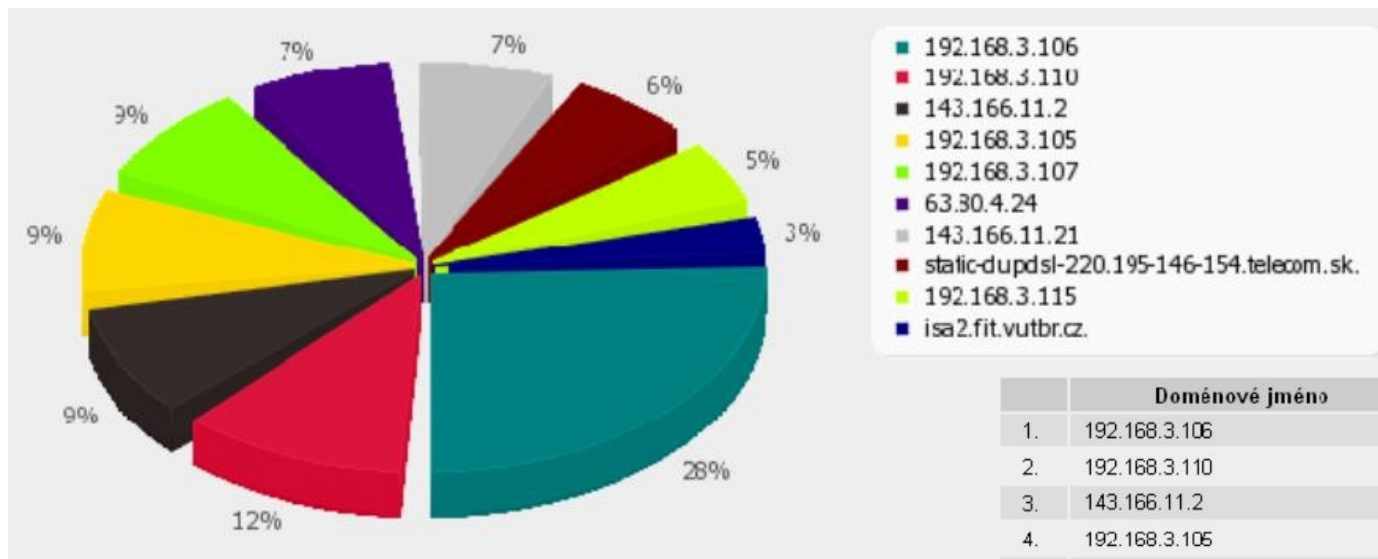


- Caligare Flow Inspector
- NetFlow Tracker
 - interaktivní grafy
 - drill-down funkcionalita
 - pokročilý reporting



Potřebujete přehledné koláčové grafy
pro manažery?

- Inteligentní reportovací nástroj, 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



	Doménové jméno	IP adresa	Bity/s	Bajty
1.		192.168.3.106	19.5 k	80.01 M
2.		192.168.3.110	3.4 k	34.62 M
3.		143.166.11.2	7.0 k	27.75 M
4.		192.168.3.105	6.3 k	26.04 M
5.		192.168.3.107	7.6 k	25.18 M
6.		63.30.4.24	1.1 M	21.27 M
7.		143.166.11.21	307.8 k	20.41 M
8.	static-dupdsl-220.195-146-154.telecom.sk	155.146.154.220	225.4 k	18.79 M
9.		192.168.3.115	3.9 k	15.64 M
10.	isa2 fit vutbr cz	147.229.176.17	2.0 k	9.35 M
Celkem			16.4 k	164.6 M

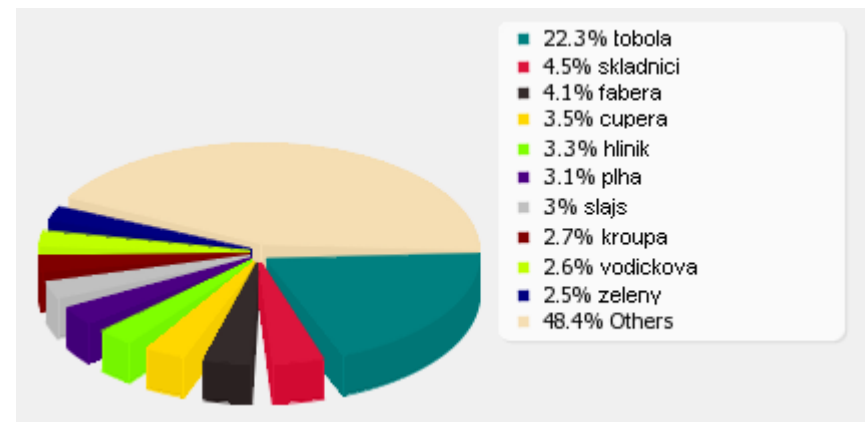
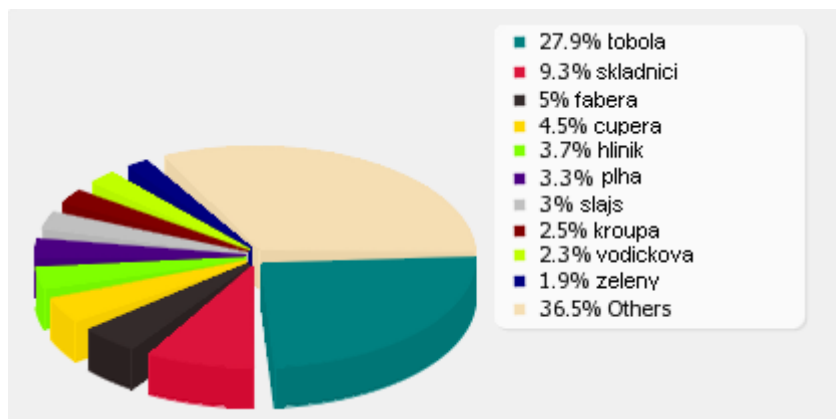
- Report pro administrátora:
 - Jak je vytížená připojovací linka k internetu?
 - Jaké se využívají jednotlivé služby v síti?
 - Kdo nejvíce vytěžuje klíčový server s IS?
 - Nejsou v komunikacích výrazné odchylky?

- Report pro manažera:
 - Kdo chodí nejvíce na web?
 - Na které weby se nejvíce chodí?
 - Kdo rozesílá nejvíce emailů?
 - Kdo je král P2P sítí?



Víte, na které weby chodí Vaši uživatelé?

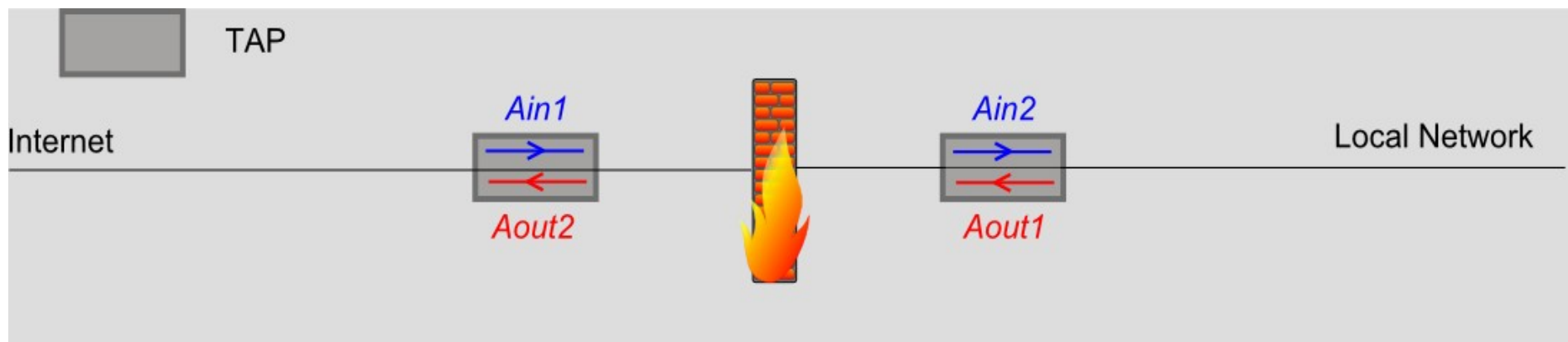
- Přehled nejnavštěvovanějších webových stránek
- Většina zaměstnanců na web vůbec nechodí..nebo?:)



Uživatel	Servery	Domény
tobola	1131	1228
	147	idnes.cz
	89	gamesy.cz
	69	www.idnes.cz
	69	freeefoto.cz
	48	www.superstar.cz
	39	42
	31	www.blesk.cz
	31	39
	31	www.invea-tech.com
31	33	
31	www.lolytky.cz	
29	31	
	suggestqueries.google.com	
	31	
	www.tipsport.cz	
	29	
	www.agi.org.uk	
	org.uk	

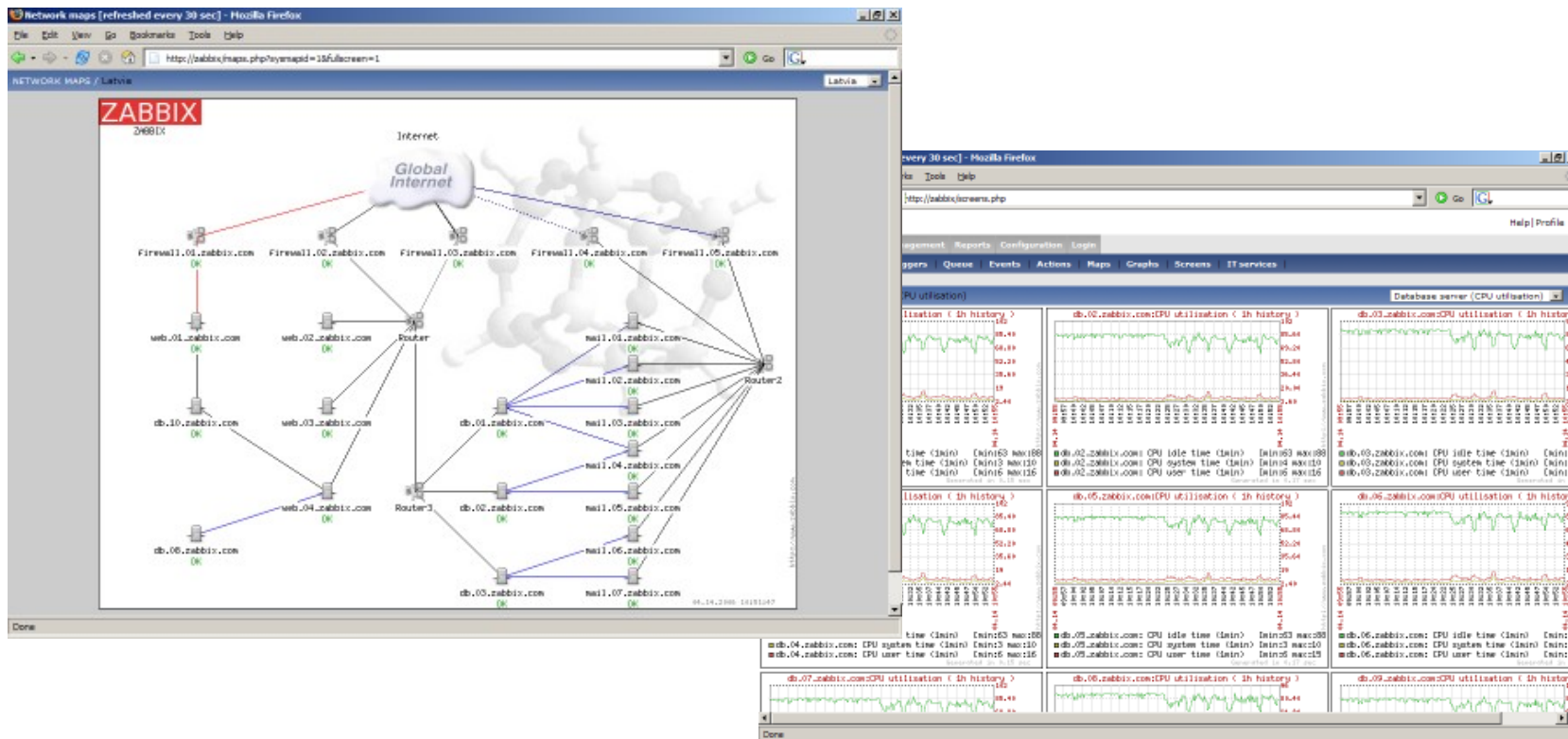
Nejste si jisti správnou konfigurací
svého firewallu?

- Nástroj pro kontrolu konfigurace a funkce firewallu
- Přehled zablokovaných toků v obou směrech
- Upozornění na toky porušující pravidla firewallu



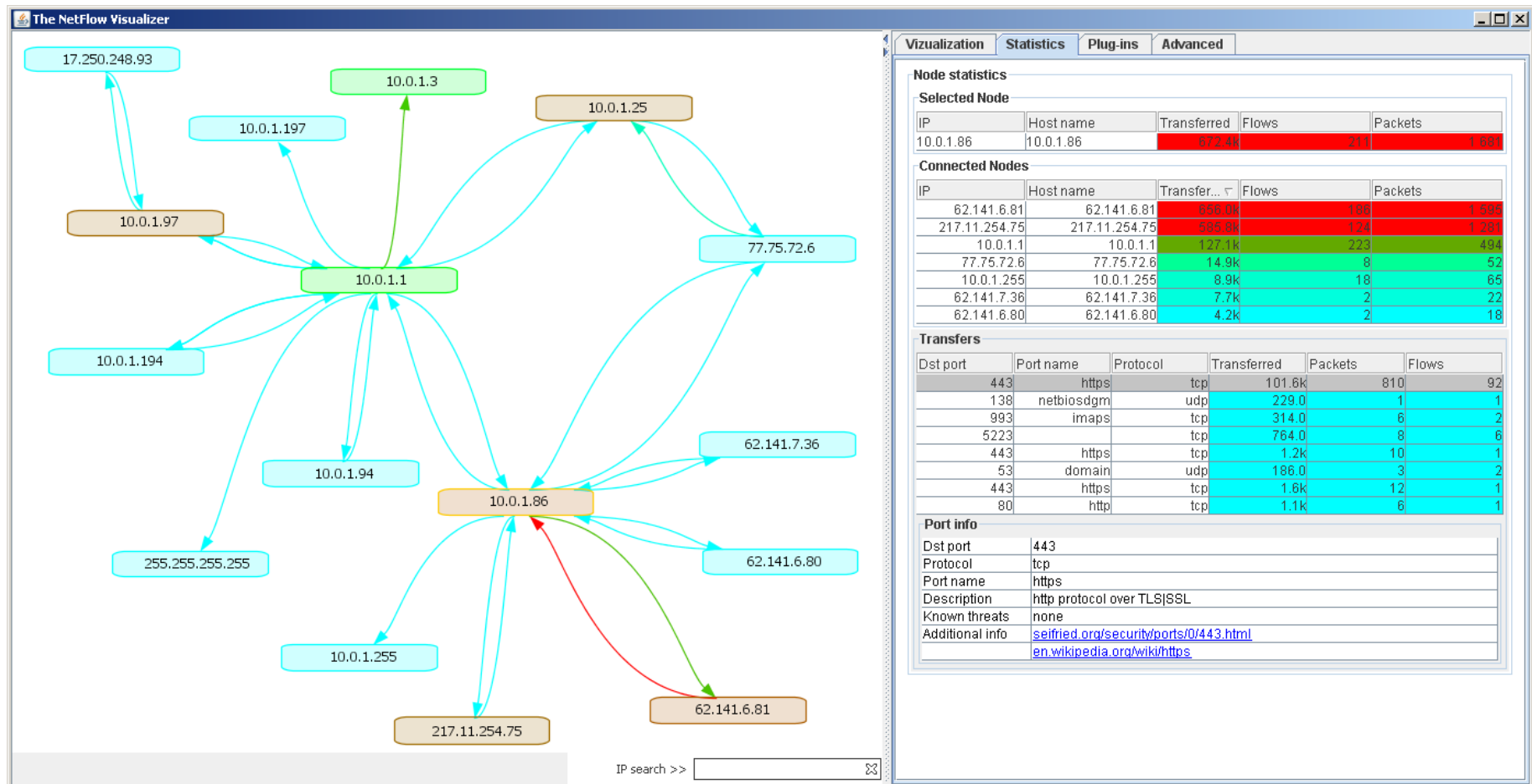
Nemáte jednoduchý nástroj pro dohled aktivních prvků, serverů a služeb?

- Dostaňte upozornění od automatického systému dříve než od šéfa / zákazníka / uživatele
- Dohled síťových prvků, serverů, služeb
- ICMP, SNMP, agenti pro monitoring místa na disku atd.

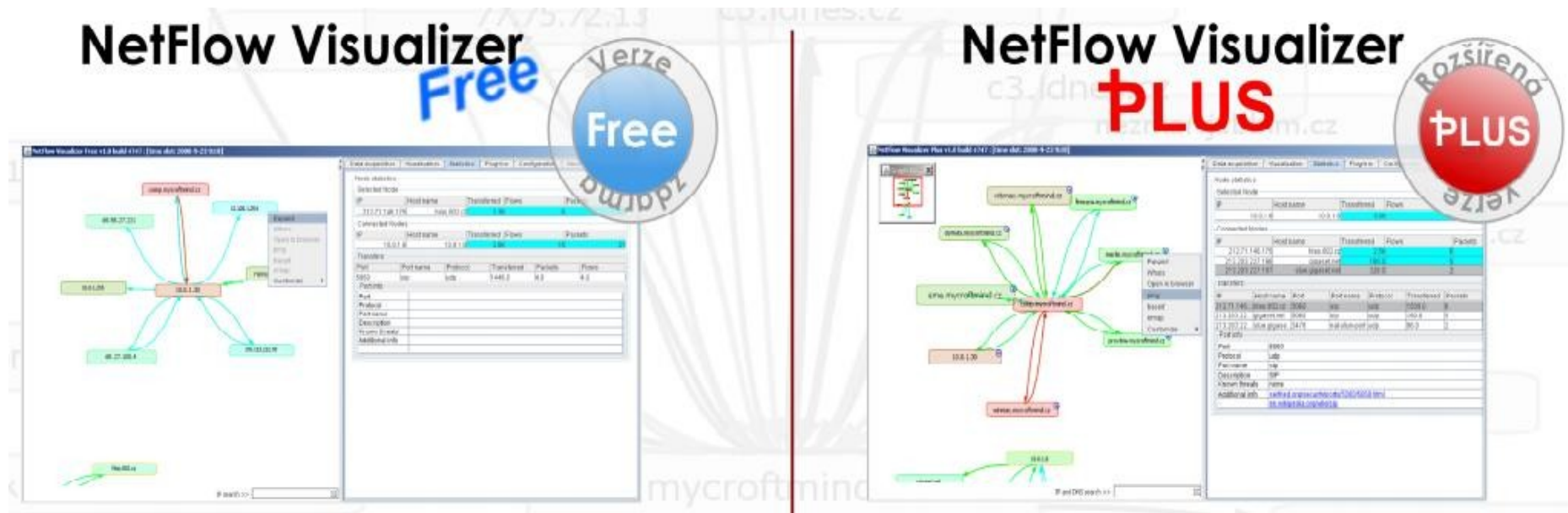


Chcete na síťové komunikace nahlížet
jednodušeji?

- Inovační technologie vizualizace NetFlow dat
- Jediný plugin běžící jako aplikace na uživatelské stanici

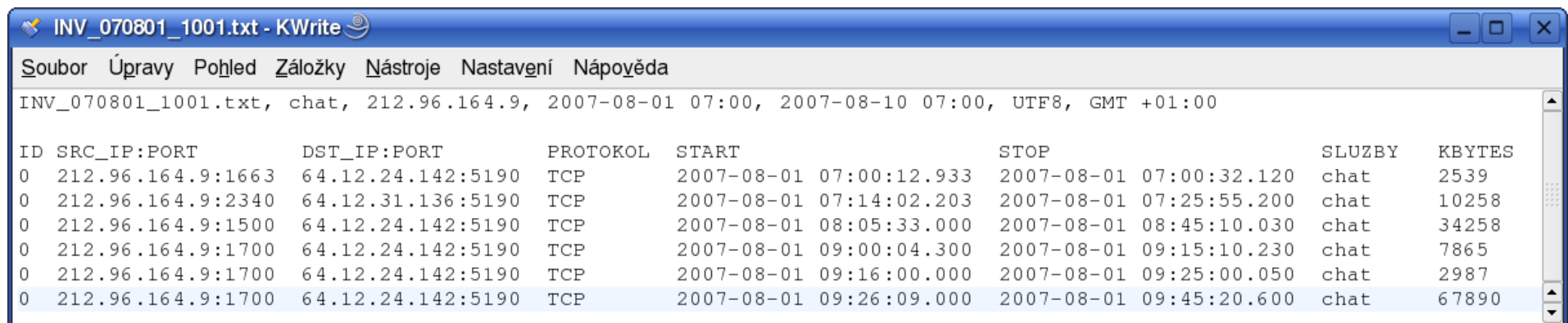


- NfVis
 - přehledné zobrazení sítě a objemů přenášených dat
 - zdarma ke každému zařízení FlowMon
- NfVis Plus
 - integrace nástrojů whois, ping, traceroute a dalších
 - pokročilejší možnosti filtrování



Nemáte splněn zákon o elektronické komunikaci 485/2005?

- Řešení vyhlášky 485/2005 (3.3.5)
- Strukturovaný výpis datové komunikace - kdo s kým kdy komunikoval a kolik přenesl dat
- Úspěšně otestováno ministerstvem vnitra

A screenshot of a KWrite window titled "INV_070801_1001.txt - KWrite". The window shows a structured log of network traffic. The log header includes file name, protocol, source IP, and time range. The main content is a table with columns for ID, SRC_IP:PORT, DST_IP:PORT, PROTOKOL, START, STOP, SLUZBY, and KBYTES. The data shows several chat sessions over TCP connections.

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

Máte neposlušné uživatele
přeprodávající konektivitu?

- Odhalení kolik uživatelů se skrývá za jednou IP adresou
- Detekce nežádoucích bezdrátových přístupových bodů

Detected NATs (Jan 7 2010 00:01 - Jan 8 2010 00:00) top			
Previous		Next	
5 Minutes		30 Minutes	1 Hour
1 Day			
IP	Host Name	No. of Masqueraded Hosts	Probability
192.168.50.9	rumcajs.raholec.cz.	12	100%
192.168.48.39	manka.raholec.cz.	8	85%
192.168.50.175	cypisek.raholec.cz.	6	100%
192.168.46.203	bob.klobouk.cz.	3	65%
192.168.42.10	bobek.klobouk.cz.	14	95%
192.168.52.239	kremilek.parezovachaloupka.cz.	9	75%
192.168.50.156	vochomurka.parezovachaloupka.cz.	7	80%
192.168.46.248	tobola.hospoda.cz.	18	100%

Tušíte, že bezpečnost Vaší vnitřní sítě
není úplně v pořádku?

- Detekce nežádoucích vzorů chování

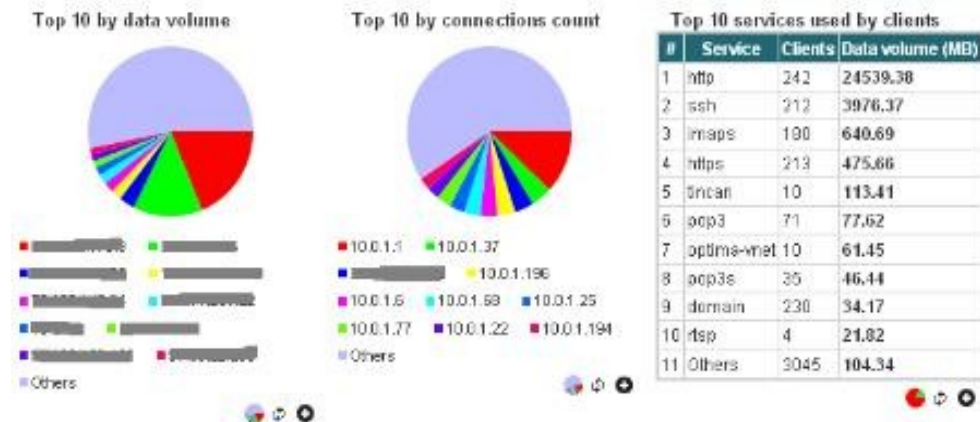
- útoky
- SPAMy, P2P aplikace
- nežádoucí služby
- provozní problémy

- Budování profilů chování

- komunikační partneři
- objemy provozu
- struktura provozu

- Detekce anomálií

- změny chování
- nové služby v síti



#	Type	Details	Timestamp	Event targets
1	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:39:50	██████████.24.5
2	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:13:42	██████████.24.5
3	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 15:59:44	██████████.24.5



FlowMon ADS

Vnější i VNITŘNÍ bezpečnost pro Vaši síť!

Jiří Tobola

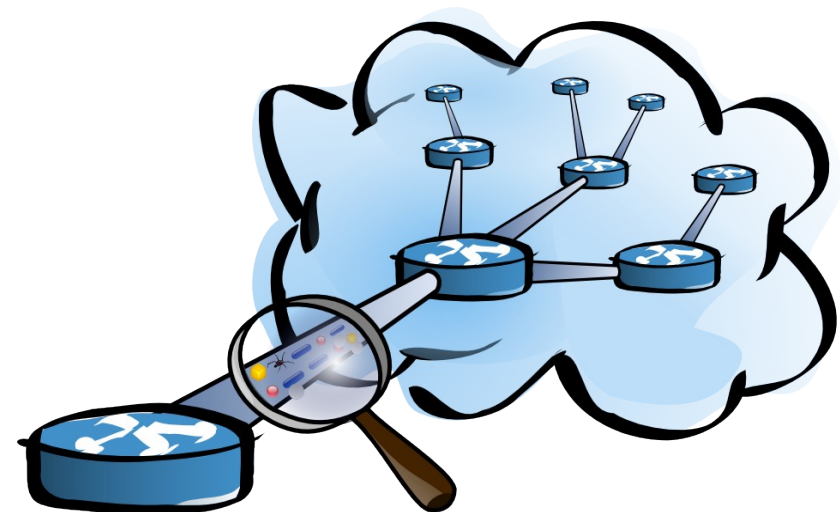
tobola@invea.cz



Váš partner ve světě vysokorychlostních sítí

- Úniky citlivých informací
- Sociální inženýrství
- Nedostupnost služeb v důsledku přetížení sítě
- Nekázeň zaměstnanců
- Dodržování autorských práv
- Nový spyware
- Zvyšující se míra šifrovaného provozu

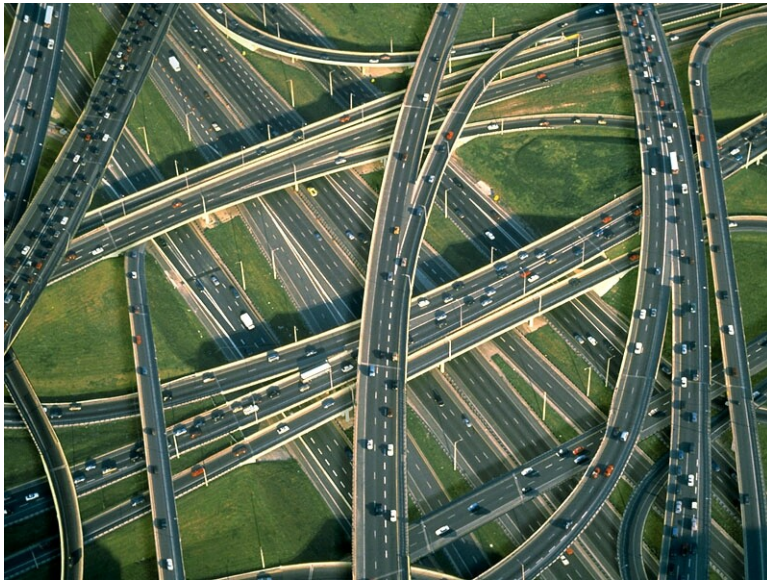
Řešení?



- Detekce nežádoucích vzorů chování
 - útoky
 - nežádoucí služby
 - provozní problémy
- Behaviorální analýza
 - profily chování
 - detekce anomálií
- Network-based řešení
 - vysoce škálovatelné
 - není třeba cokoliv instalovat na koncových stanicích
 - nová zařízení v síti jsou automaticky monitorována



Detekce chování

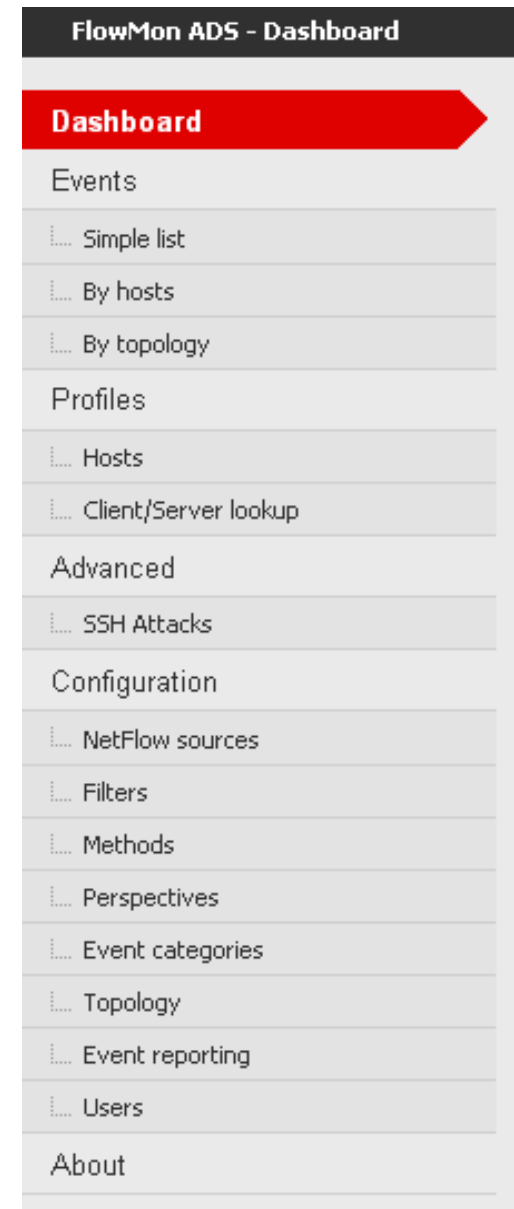


Detekce obsahu

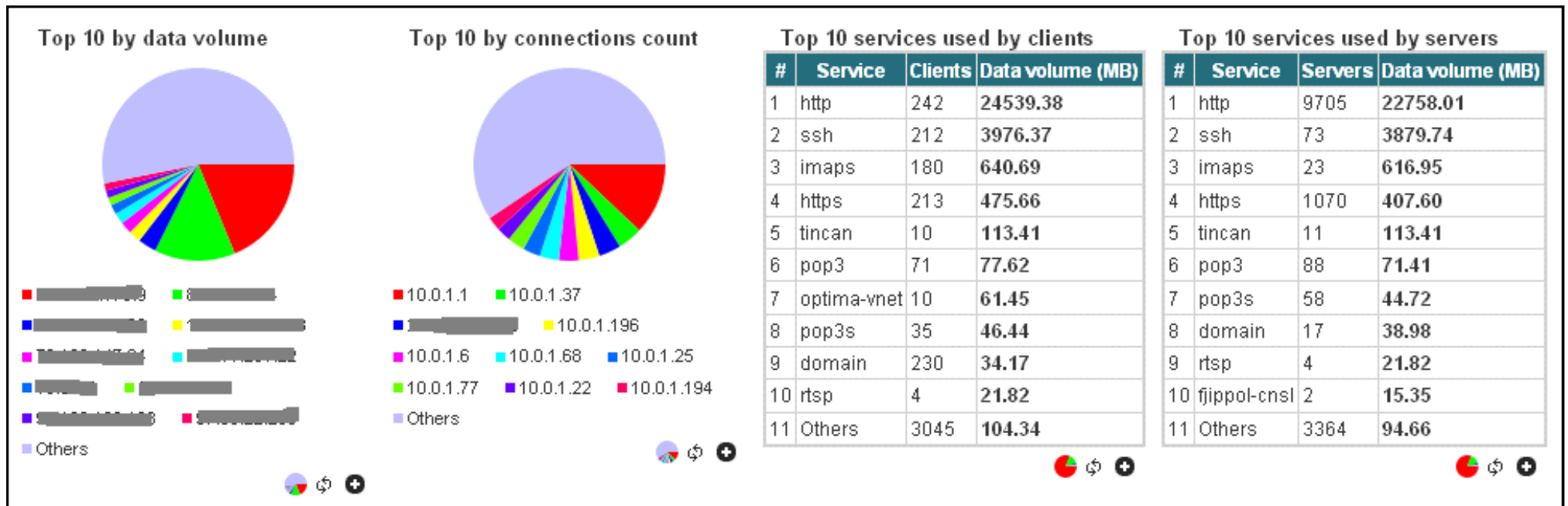


- Detekuje podezřelé chování, které je nezjistitelné jinými systémy
- Použitelné v šifrovaném provozu
- Reaguje na neznáme hrozby

- Moderní webové uživatelské rozhraní
 - využití technologie AJAX
 - kontextové menu pro rychlý pohyb v UI
- Integrace dalších informací
 - DNS
 - WHOIS
- Řada alternativních pohledů na události
 - dashboard
 - prostý seznam
 - pohled přes IP adresy
 - pohled přes topologii



- Okamžitá indikace problémů v síti
- Přehled nových/prioritních událostí
- Grafická reprezentace



- Slovníkové útoky
 - rozpoznání slovníkového útoku na službu SSH
 - vyhodnocení úspěšnosti útoku
 - ochrana serverů

SSH Attacks

Successful attacks in result: **0**

Non-successful attacks in result: **11**

#	Timestamp	Attacker	Victim	Attack status	Certainty (%)
1	2009-09-16 20:07:37	144.16.112.114	██████████.65.2	non-success	100.00
2	2009-09-16 20:07:32	144.16.112.114	██████████.65.55	non-success	100.00
3	2009-09-16 20:06:37	144.16.112.114	██████████.80.252	non-success	100.00

- P2P síť
 - odhalování využívání peer-to-peer sítí ke sdílení a stahování dat
 - Bit Torrent, DC++
 - dohled na využitím sítě a její optimalizace
 - dodržování autorských práv

Events

██████████ 8.122

#	Type	Details	Timestamp	Event targets
1	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:39:50	██████████.24.5
2	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 16:13:42	██████████.24.5
3	BITTORRENT	BitTorrent downloads, unique sources: 1	2009-09-24 15:59:44	██████████.24.5

- Nadměrné přenosy dat
 - dohled nad využíváním přenosové kapacity sítě
 - odhalování uživatelů, kteří nadměrně zatěžují síť

Events

██████████144.133

#	Type	Details	Timestamp	Event targets
1	HIGHTRANSF	transferred: 106112952 B	2009-09-09 06:38:02	

██████████24.2

#	Type	Details	Timestamp	Event targets
10	HIGHTRANSF	transferred: 15848830 B	2009-09-09 06:28:47	

- SPAM

- odhalování pokusů o spamování z hlídané sítě
- využívání neautorizovaných SMTP serverů
- detekce napadených počítačů v síti

Events

#	Event source	Type	Details	Timestamp	Data source	Event targets
1	██████████ 67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 7)	2009-09-24 19:23:00	PřF	62.3.131.181, 69.7.167.23, 146.201.3.234, 194.109.24.132, 209.145.5.10, 210.101.199.231, 213.232.0.195
2	██████████ 67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 65)	2009-09-24 19:17:45	PřF	62.3.131.181, 63.101.151.1, 64.18.4.11, 64.18.5.10, 64.18.6.10, 64.18.6.14, 64.18.7.13, 64.191.223.42, 65.55.88.22, 65.172.13.10, ...
3	██████████ 67.145	OUTSPAM	SMTP [TCP:25] (unique hosts: 75)	2009-09-24 19:16:00	PřF	62.12.136.97, 63.166.155.140, 64.18.6.10, 64.18.6.11, 64.18.7.11, 64.26.60.153, 64.88.167.155, 64.118.228.132, 65.55.88.22, 65.61.115.199, ...

- Skenování portů/DoS útoky
 - odhalování TCP skenů, které typicky předchází cíleným útokům
 - rozpoznání horizontálních i vertikálních skenů
 - odhalování zahlcování serverů (DoS a DdoS útoky)

Events

████████.26.47

#	Type	Details	Timestamp	Event targets
1	SCANS	TCP SYN scan (attempts: 2188)	2009-09-25 01:25:50	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
2	SCANS	TCP SYN scan (attempts: 2874)	2009-09-25 01:25:50	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.6, ██████████.24.7, ██████████.24.8, ██████████.24.9, ...
3	SCANS	TCP SYN scan (attempts: 79)	2009-09-24 20:27:26	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
4	SCANS	TCP SYN scan (attempts: 406)	2009-09-24 15:54:27	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
5	SCANS	TCP SYN scan (attempts: 1041)	2009-09-24 10:26:47	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
6	SCANS	TCP SYN scan (attempts: 1238)	2009-09-24 10:26:47	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
7	SCANS	TCP SYN scan (attempts: 3925)	2009-09-24 05:13:22	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...
8	SCANS	TCP SYN scan (attempts: 93)	2009-09-24 05:13:22	████████.24.0, ██████████.24.1, ██████████.24.2, ██████████.24.3, ██████████.24.4, ██████████.24.5, ██████████.24.12, ██████████.24.14, ██████████.24.15 ██████████.24.16, ...

- Zpoždění sítě
 - rozpoznání enormního zpoždění na úrovni sítě
 - diagnostika provozních problémů (aplikace/sítě)
 - optimalizace sítě

Events

██████████ 24.2

#	◆ Type	◆ Details	◆ Timestamp	▼ Event targets
2	LATENCY	latency: 933 ms	2009-09-09 06:37:49	██████████.184.64

██████████ .27.201

#	◆ Type	◆ Details	◆ Timestamp	▼ Event targets
6	LATENCY	latency: 911 ms	2009-09-09 06:37:31	██████████.199.176

- Instant Messaging
 - odhalování využívání služeb instant messagingu jako je ICQ, Jabber, Google Talk apod.
 - ochrana pracovní kázně
 - zvýšení produktivity práce

Events

██████████.36.2

#	Type	Details	Timestamp	Event targets
1	INSTMSG	OSCAR protocol, unique servers: 1	2009-09-25 03:53:46	██████████.82.5
2	INSTMSG	OSCAR protocol, unique servers: 1	2009-09-24 23:31:45	██████████.80.11
3	INSTMSG	OSCAR protocol, unique servers: 1	2009-09-24 16:55:47	██████████.82.5

- Reverzní DNS záznamy
 - Odhalování zařízení bez reverzních záznamů
 - Indikace neautorizovaných zařízení/konfiguračních problémů
 - Kombinace s profily chování – např. webové servery bez reverzního DNS záznamu

Hosts without reverse DNS record

#	↕	IP address	↕	Date
1		10.0.1.8		2009-12-21
2		10.0.1.9		2009-12-21
3		10.0.1.222		2009-12-21

- Budování profilů chování zařízení na síti
 - serverové a klientské chování
 - objemy provozu
 - komunikační partneři
 - struktura provozu (poskytované a využívané služby)
- Využití
 - analýza sítě
 - odhalování serverů a klientů v síti
 - detekce nových služeb v síti
 - databáze komunikujících strojů

Client/Server behavior

#	Client (%)	Server (%)	Unclassified (%)
1	48.84	23.38	27.78

- Základní principy
 - porovnání profilu chování vůči automaticky naučené baseline
 - reportování anomálie v případě významné odchylky formou standardní události
- Rozpoznávané anomálie
 - změna serverového/klientského chování zařízení
 - změna v objemech provozu spojených s daným zařízením
 - změna v rozsahu využívání nebo poskytování služby
 - změna počtu komunikačních partnerů



- V etapě implementace
 - nasazení s okamžitým efektem
 - odpadá složitá konfigurace a ladění zařízení řešením
 - pro síť s cca 1000 počítači konfigurace do 30ti minut
- Při běžném použití
 - automatizace řady postupů dohledu sítě
 - nízké nároky na odbornou kvalifikaci obsluhy
- Příklad – odhalování skenování
 - ruční vyhledávání na základě špiček v grafech a následné dotazování na toky daných vlastností
 - automatická detekce skenů a následné upozornění



- Monitoring jako prostředek ochrany
 - běžná bezpečnostní opatření bývají obcházena, síťový monitoring obejít nelze
 - skutečnost, že je síť detailně monitorována vede k jejímu nižšímu zneužívání uživateli
- Příklady
 - dohled nad využitím sítě zaměstnanci (P2P, přenosy dat, ...)
 - odhalování používání nežádoucích služeb (ICQ a jiné instant messengery)



- Komplexní analýza chování na síti
 - události, profily, statistika využívaných a poskytovaných služeb
 - permanentní dohled nad rutinním provozem sítě
- Přímé upozornění na bezpečnostní hrozby
 - včasné odhalení a reportování útoků
 - obecný mechanismus detekce anomálií v síti
 - detekce nových služeb a trendů v chování sítě
- Doplněk
 - firewallů
 - IDS/IPS sond
 - antivirů
 - antimalware řešení



- 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





Váš partner ve světě vysokorychlostních sítí

Jiří Tobola

tobola@invea.cz

602 647 684

INVEA-TECH a.s.

U Vodárny 2965/2

616 00 Brno

www.invea.cz

