Flow Monitoring & NBA

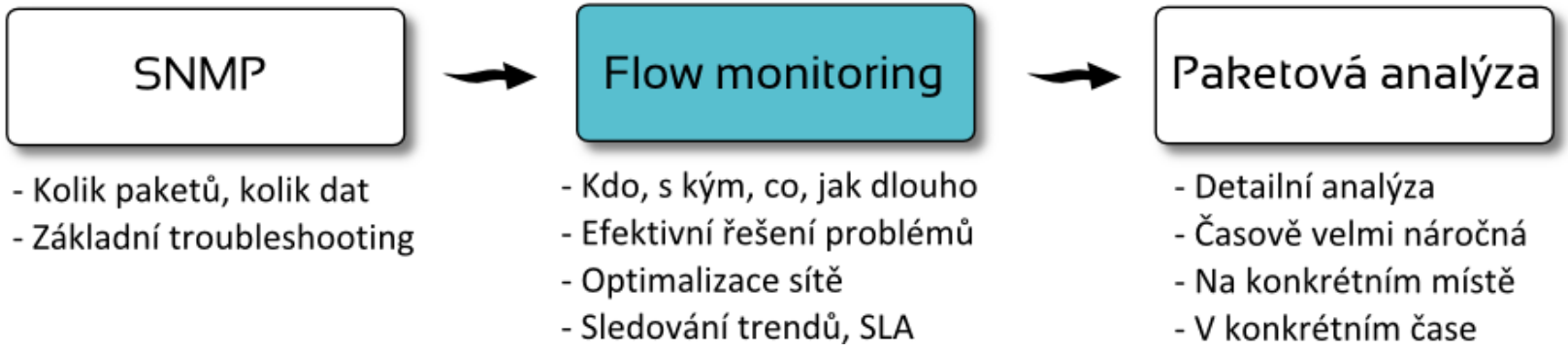
Pavel Minařík
minarik@invea.cz

Formulace zadání

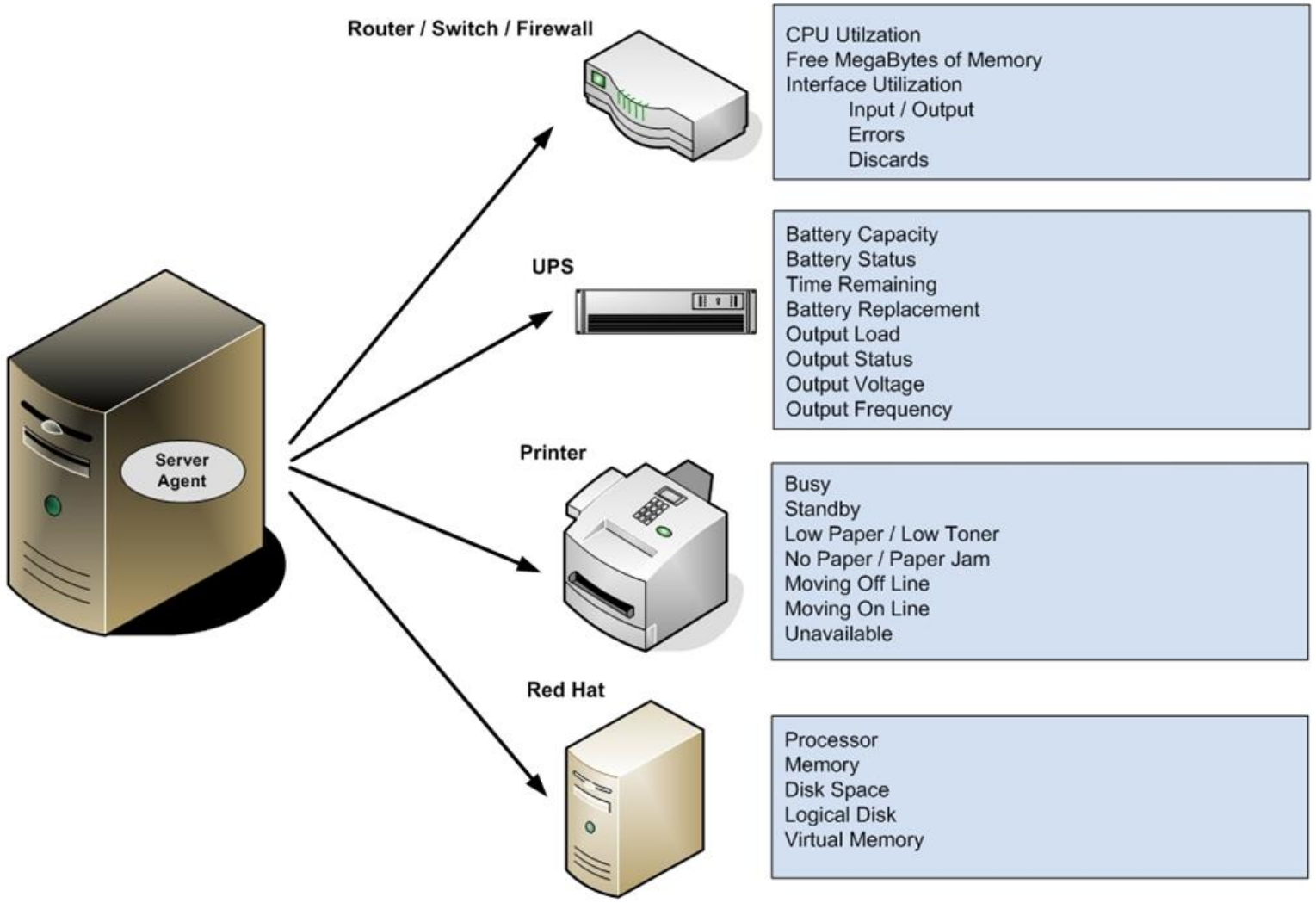
- Zákazník požaduje řešení pro monitorování a analýzu provozu datové sítě
  - Měření provozu v prostředí multi-10Gbps infrastruktury
  - Historie 1 rok zpětně s možností data analyzovat až na úroveň jednotlivých spojení
  - Reportování a přehled dle segmentů, IP, portů, protokolů, atd.
  - Automatická analýza v reálném čase a identifikace útoků, malware, potenciálních úniků dat
  - Identifikace nežádoucích aplikací a to i šifrovaných

Monitoring sítě - možnosti

- SNMP
  - pouze na úrovni základních čítačů, chybí detailní informace
- **Monitoring toků**
  - detailní přehled o dění v síti
- Paketová analýza
  - velmi detailní, ale časově velmi náročná

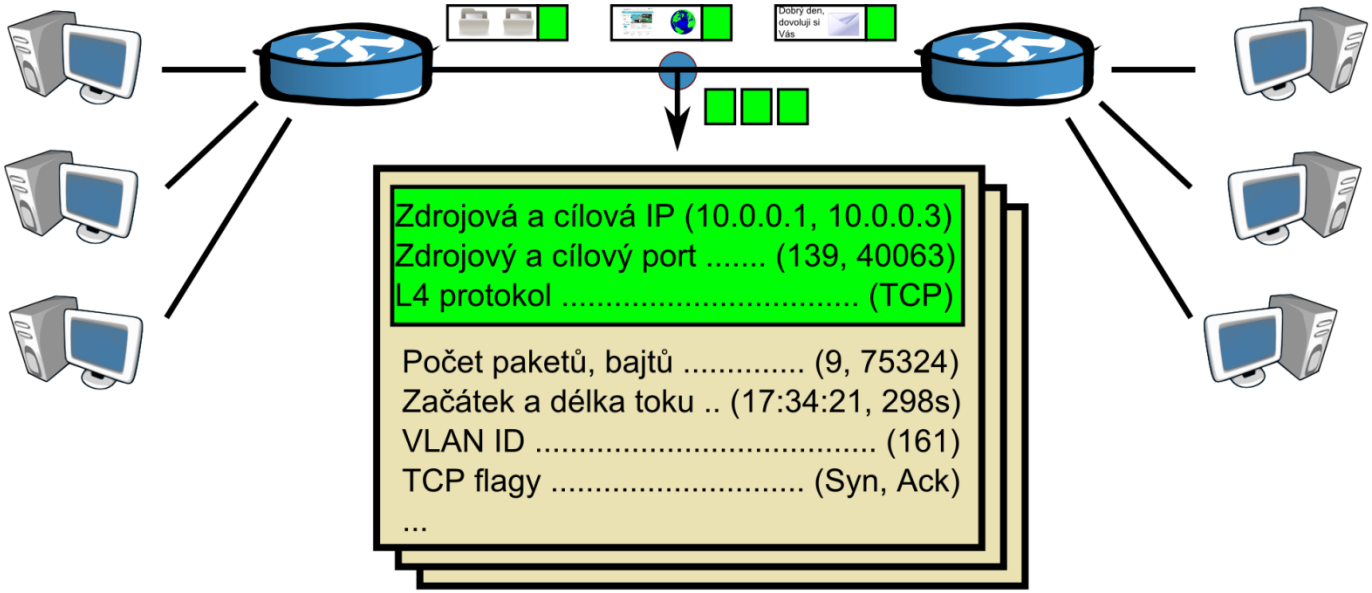


SNMP


Router / Switch / Firewall
CPU Utilzation
Free MegaBytes of Memory
Interface Utilization
Input / Output
Errors
Discards
UPS
Battery Capacity
Battery Status
Time Remaining
Battery Replacement
Output Load
Output Status
Output Voltage
Output Frequency
Server Agent
Printer
Busy
Standby
Low Paper / Low Toner
No Paper / Paper Jam
Moving Off Line
Moving On Line
Unavailable
Red Hat
Processor
Memory
Disk Space
Logical Disk
Virtual Memory

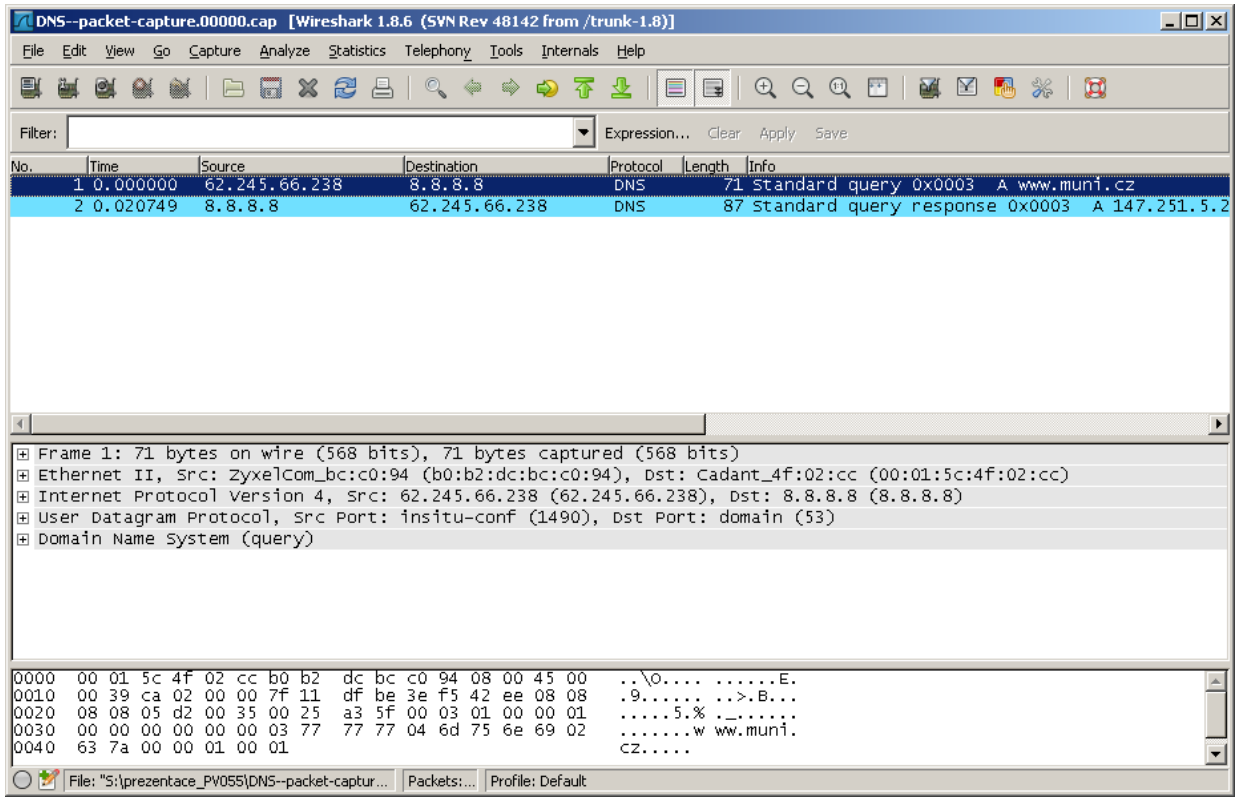
Flow Monitoring

- Měření na základě IP toků
- Analyzují se pouze hlavičky paketů, obsah paketů není monitorován ani uchováván
- Moderní metoda monitorování sítí, Cisco standard v5/v9
- Redukce dat cca 500:1



Packet Analysis

- Zachycení provozu v plném rozsahu, vč. obsahu
- Extrémní požadavky na výkon a diskovou kapacitu
- Nástroje
  - tcpdump
  - Wireshark
  - …



Moderní hrozby

- APT (Advanced Persitent Threats)
- Zero-day útoky a polymorfní malware
- Postranní komunikační kanály

- Společné rysy
  - Často šité na míru cílovému prostředí
  - Neexistují signatury nebo nejsou dostupné včas
  - Neviditelné pro běžné bezpečnostní nástroje


eurostat newsrelease

21/2011 - 7 February 2011

8 February 2011: Safer Internet Day

Nearly one third of internet users in the EU27 caught a computer virus

84% of internet users use IT security software for protection


IT Security & Network Security News

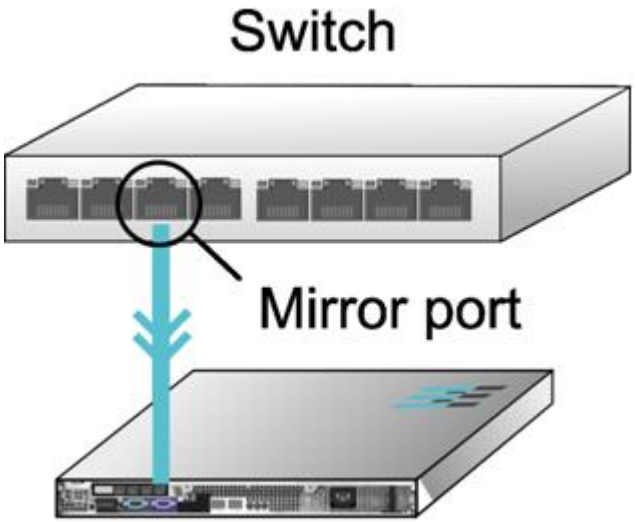
Japan's Largest Defense Contractor Hit by Cyber-Attackers

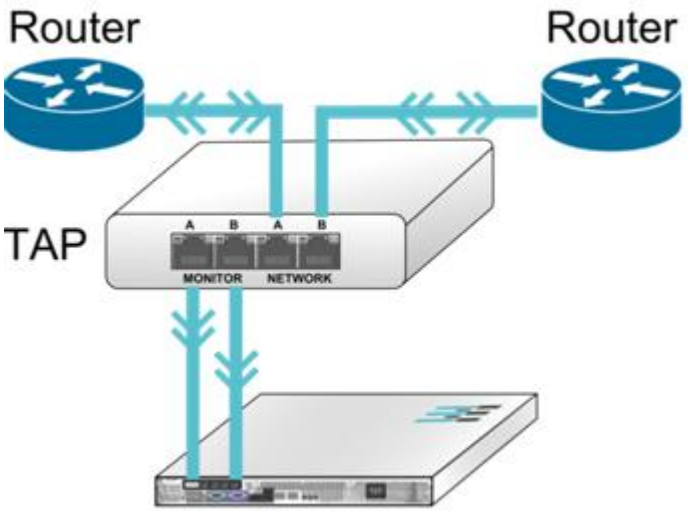
LinkedIn Twitter 5 Facebook 3 +1 0 Share 8

By: Fahmida Y. Rashid
2011-09-19
Article Rating: ☆☆☆☆☆ / 0

Měření provozu

- Jak technicky provoz sledovat
  - Inline
  - SPAN/mirror
  - TAP





Ukládání provozu

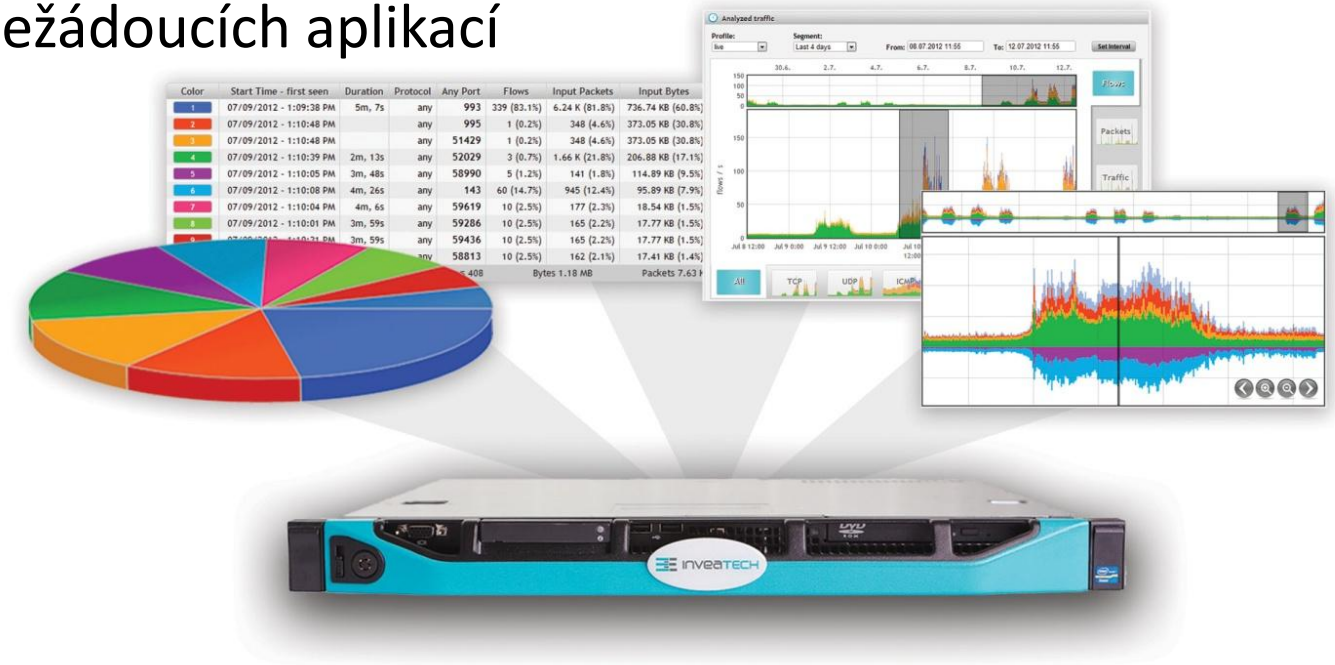
- SNMP
  - Nevyhovuje, pouze objemy, nepoužitelné

1Gbps linka vytížená na 10%	Paketová analýza	Flow monitoring
Disková kapacita na 1 den provozu	Cca 1TB	Cca 2 GB
Propustnost měřícího systému	Stejná jako měřený provoz	Stejná jako měřený provoz, ale zpracují se jen hlavičky
Propustnost úložiště a analytického systému	100Mbps, stejná jako měřený provoz	cca 200kbps

Splnění požadavků

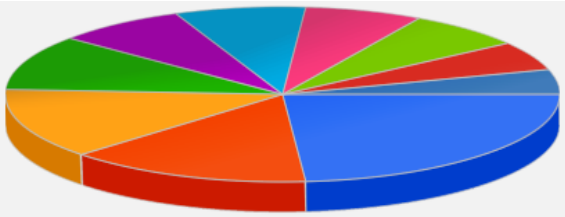
Provozní i bezpečnostní využití

- Struktura a charakter provozu
- Identifikace provozních problémů a jejich příčin
- Odhalování infikovaných stanic, útoků a pokročilých hrozeb
- Odhalování nežádoucích aplikací

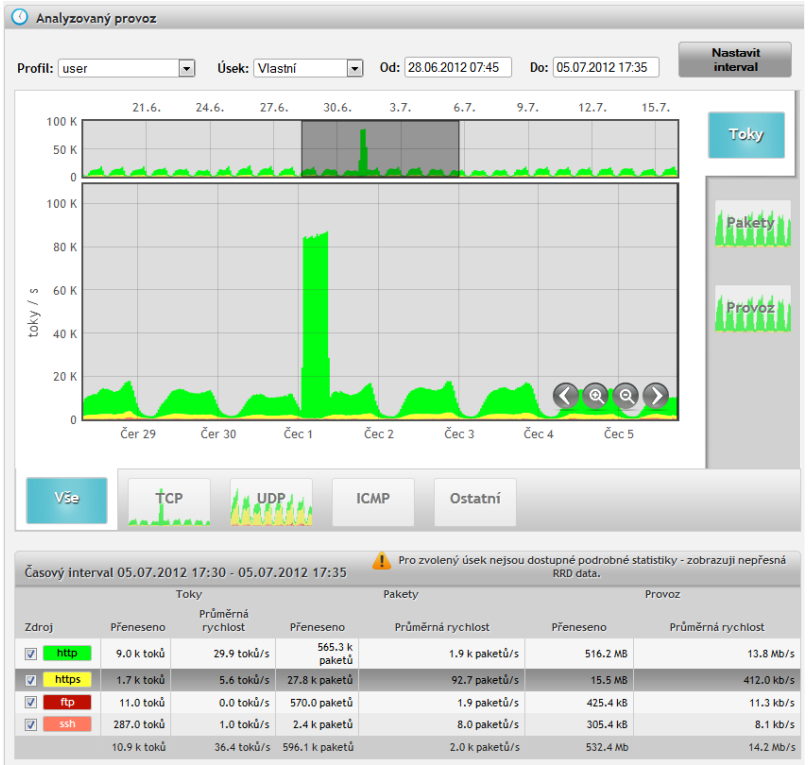


Struktura a charakter provozu

- 10% uživatelů typicky vygeneruje 90% provozu – kteří to jsou?
- Jak jsou využívány služby a proč byla včera síť tak pomalá?

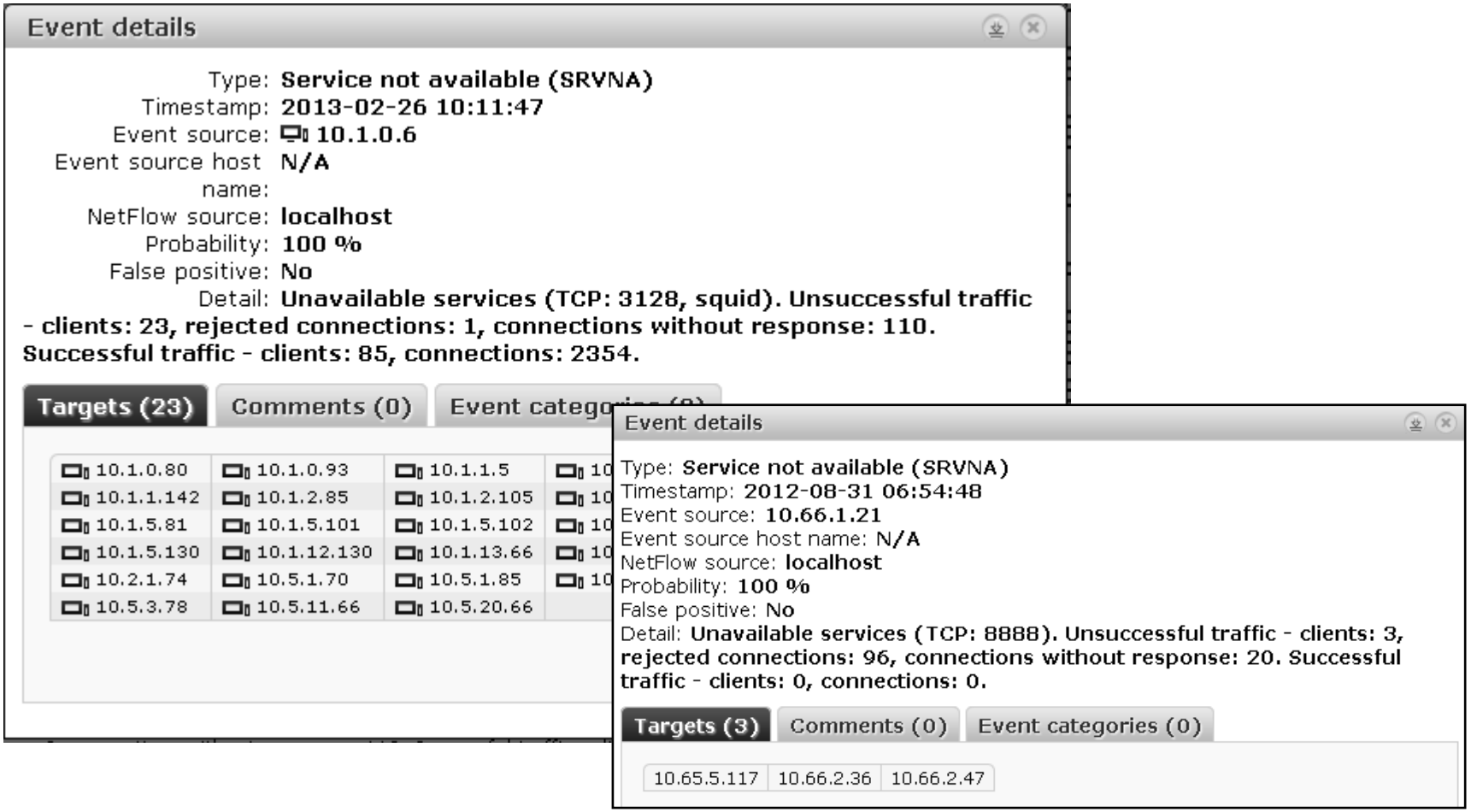


Barva	Počáteční čas	Trvání	Protokol	Statistika	Toky
1	22.5.2012 7:00:12	52,476	všechny	192.168.3.254	93.89 K (22.9%)
2	22.5.2012 6:58:09	52,607	všechny	192.168.17.5	56.03 K (13.7%)
3	22.5.2012 7:38:38	49,954	všechny	192.168.27.254	51.5 K (12.6%)
4	22.5.2012 8:04:44	48,580	všechny	192.168.15.254	40.29 K (9.8%)
5	22.5.2012 6:59:42	52,518	všechny	192.168.6.255	30.75 K (7.5%)
6	22.5.2012 9:31:02	41,617	všechny	192.168.27.151	30.24 K (7.4%)
7	22.5.2012 7:00:10	52,486	všechny	192.168.17.212	27.94 K (6.8%)
8	22.5.2012 6:58:09	52,606	všechny	192.168.17.211	27.82 K (6.8%)
9	22.5.2012 8:07:41	48,403	všechny	192.168.15.111	21.64 K (5.3%)
10	22.5.2012 7:00:24	52,445	všechny	255.255.255.255	18.55 K (4.5%)



Provozní problémy a příčiny

- Chybné konfigurace a výpadky služeb



Neznámý malware

TIME Techland
News and reviews about gadgets, gear, apps and the web

Home | Gadgets | Apps & Web | News | Reviews & Features | Companies

SECURITY

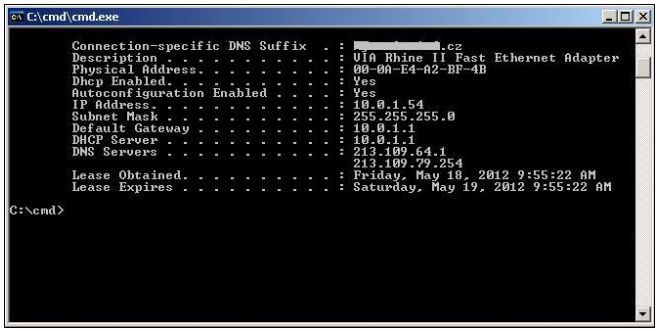
DNSChanger: FBI Warns Infected Computers Will Lose Web, I Access in July

By MATT PECKHAM | @mattpeckham | April 23, 2012 | 8

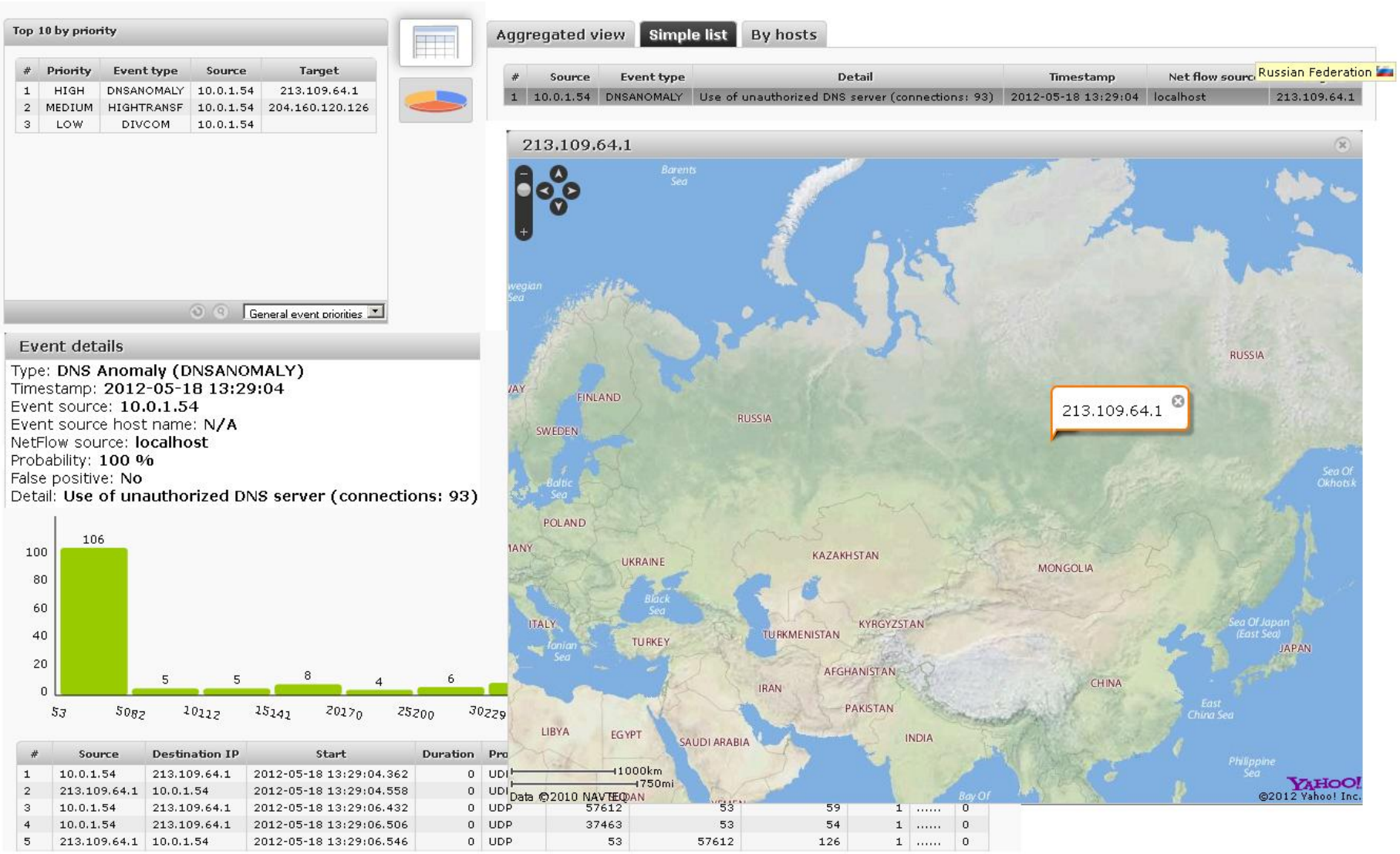
Summary

DNSChanger is a trojan that will change the infected system's Domain Nam traffic to unsolicited, and potentially illegal sites.

The trojan is usually a small file (about 1.5 kilobytes) that is designed to cha custom IP address. This IP address is usually encrypted in the body of a troj computer will contact the newly assigned DNS server to resolve names of di



Neznámý malware



Útoky

29 August 2011, 13:27

« previous | next »

Worm spreads via Windows Remote Desktop

Anti-virus software vendor F-Secure is warning of a piece of malware by the name of Morto, which spreads using Windows' Remote Desktop Server (RDP server). It does not exploit a Windows security vulnerability; instead, it scans IP address ranges for RDP port 3389 and then tries to log in as an administrator to any computers which respond using a list of common passwords.

Event details

Type:	**RDP Dictionary Attacks (RDPDICT)**
Timestamp:	**2013-01-25 10:48:10**
Event source:	**202.105.183.89**
Event source host name:	**N/A**
NetFlow source:	**localhost**
Probability:	**100 %**
False positive:	**No**
Detail:	**Continuation of attack, total count of targets: 1, current maximal transfer: 4.32 KiB, current count of attempts: 17. Part of distributed attack.**

Targets (1) | Comments (0) | Event categories (0)

[redacted].224.178

Úniky dat

Malware from Peru Reportedly was sending AutoCAD Drawings to China

by SUNITHBABU (ONLINE) *on* JUNE 26, 2012

Event details

Type: **Behavior Profiling - Country reputation (PRFCOUNTRY)**
Timestamp: **2013-01-25 14:43:23**
Event source: **192.168.3.149**
Event source host name: **N/A**
NetFlow source: **[redacted]cz**
Probability: **100 %**
False positive: **No**
Detail: **Unusual communication to the country Israel (device: upload: 1.01 MiB, download: 390.99 KiB, upload/download ratio: 2.63; network average: upload: 137.72 KiB, download: 263.57 KiB, upload/download ratio: 0.52).**

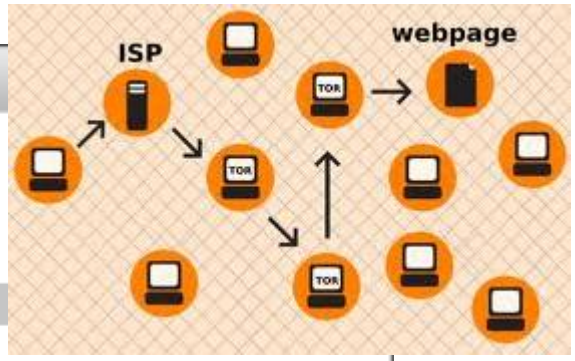
Targets (1) | Comments (0) | Event categories (0)

[redacted].77.198

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.1.1.84	UPLOAD	Uploaded: 38.83 MiB, downloaded: 0.57 MiB, ports: 80	2012-05-10 11:43:34	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
2	10.1.1.84	UPLOAD	Uploaded: 243.48 MiB, downloaded: 4.07 MiB, ports: 80	2012-05-10 11:37:19	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
3	10.1.1.84	UPLOAD	Uploaded: 199.97 MiB, downloaded: 4.49 MiB, ports: 80	2012-05-10 11:33:47	localhost	98.13[redacted] United States vip.ac4.yahoo.net)
4	10.1.1.84	UPLOAD	Uploaded: 232.03 MiB, downloaded: 4.38 MiB, ports: 80	2012-05-10 11:28:32	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)
5	10.1.1.84	UPLOAD	Uploaded: 197.11 MiB, downloaded: 3.74 MiB, ports: 80	2012-05-10 11:24:10	localhost	98.136.145.156 (r5.ycpi.vip.ac4.yahoo.net)

Nežádoucí aplikace

- **The Onion Router**
  - Klient pro různé OS
  - Nevyžaduje zvláštní schopnosti
  - Není možné detekovat analýzou obsahu
  - Vhodné pro obcházení politik a omezení



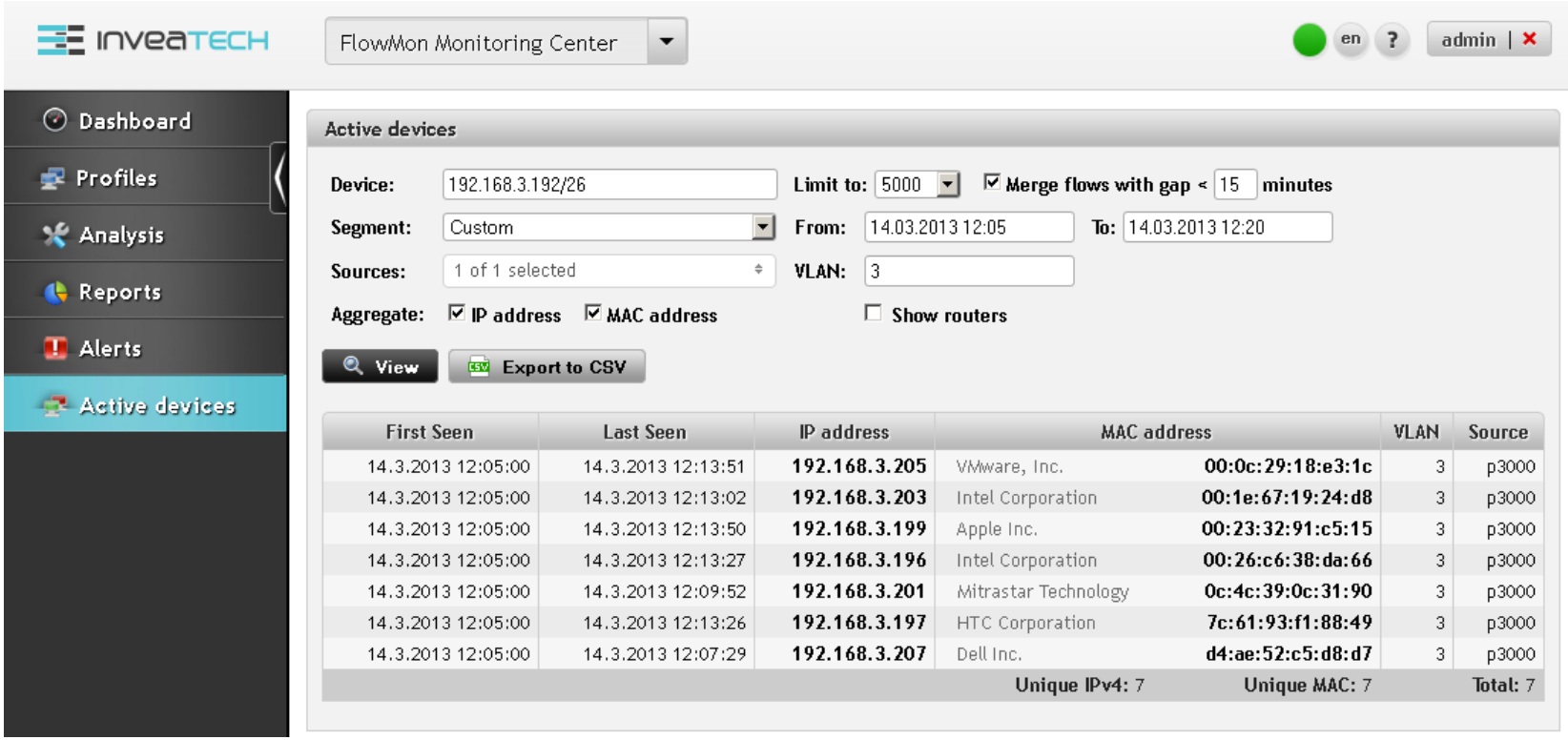
Event details

Type: **The Onion Router (TOR)**
Timestamp: **2012-05-09 13:06:59**
Event source: **10.0.1.25**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **75 %**
False positive: **No**
Detail: **Tor communication, unique onion routers: 51**

#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	10.0.1.25	TOR	Tor communication, unique onion routers: 51	2012-05-09 13:06:59	localhost	3:.31.74.162, 38.229.70.61, 46.165.196.73, 46.166.147.126, 50.7.240.10, 50.115.125.54, 62.75.186.116, 62.220.136.253, 70.33.208.83, 74.125.232.246, , ...

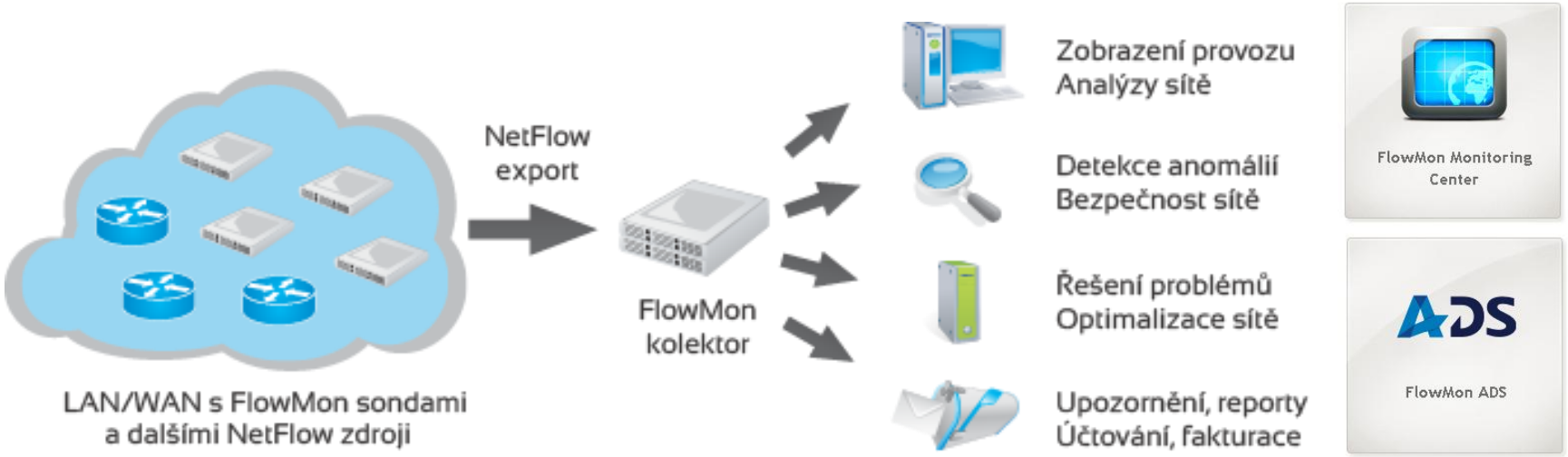
Podpora konceptu BYOD

- Monitorování aktivních zařízení v síti
- Sledování přiřazení IP adresa – MAC adresa
- Identifikace výrobce zařízení



Architektura řešení

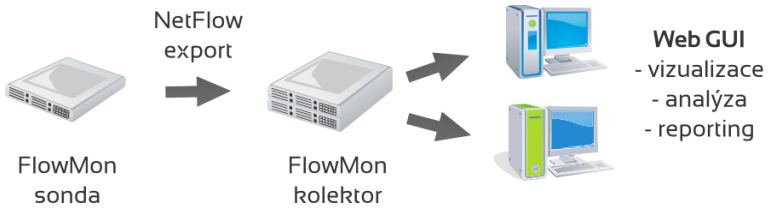
- Pasivní FlowMon sondy
  - zdroj síťových statistik (NetFlow dat)
- Kolektory NetFlow dat
  - vizualizace a vyhodnocení síťových statistik
- FlowMon ADS
  - detekce bezpečnostních událostí a anomálií

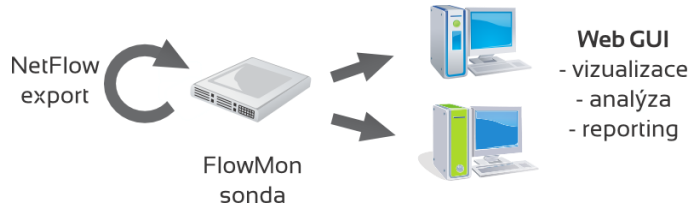


FlowMon sondy

- 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
- Vzdálená konfigurace přes intuitivní webové rozhraní
- Podpora 10/100/1000 Ethernetu, 10 GE, IPv4, IPv6, VLAN, MPLS

- Vestavěný kolektor pro okamžité uložení a analýzu dat



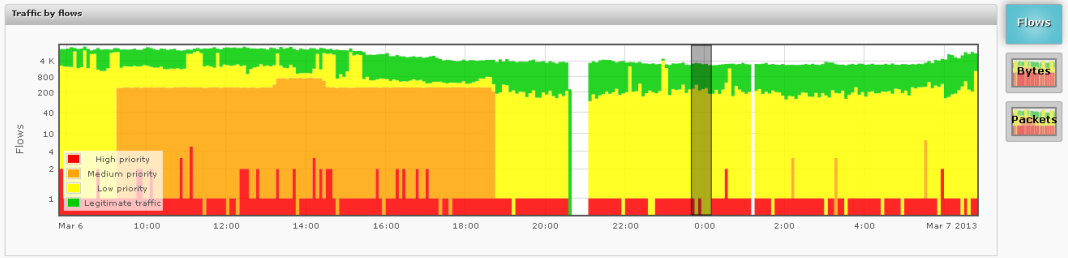


FlowMon kolektory

- Dlouhodobé uložení síťových statistik z několika zdrojů
- Kolektorová aplikace pro analýzu NetFlow/IPFIX/sFlow statistik – FlowMon Monitorovací Centrum
  - vždy v ceně zařízení
- Zobrazení a analýzy síťového provozu
- Profesionální řešení pro větší sítě
  - RAID, redundantní napájení, úložná kapacita 1 TB – 100 TB
  - dohled nad sítí z centrálního bodu v síti

FlowMon ADS

- Řešení pro automatickou analýzu provozu datové sítě
- Určeno k detekci provozních a bezpečnostních problémů a podezřelých aktivit

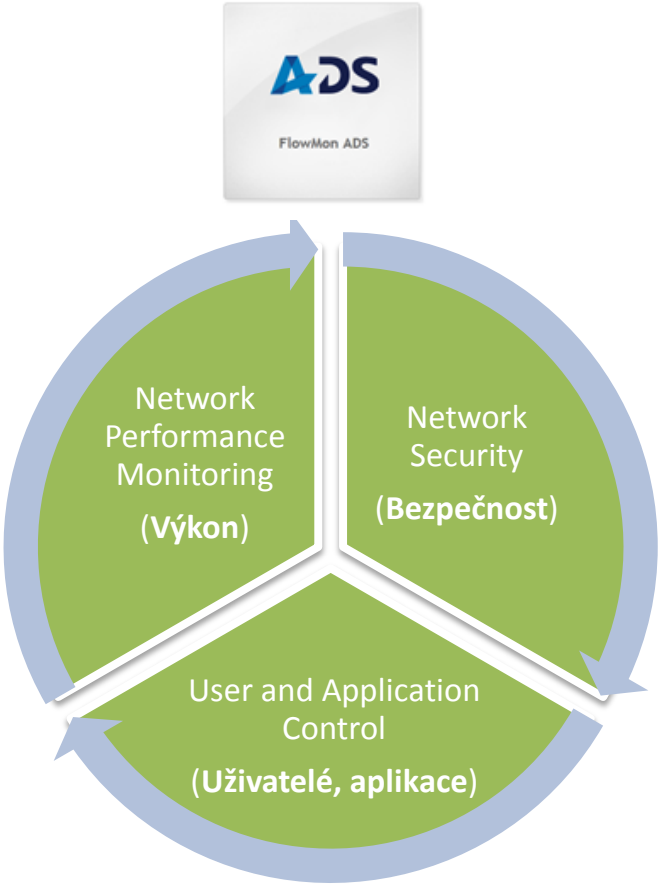


Traffic statistics (2013-03-06 23:40 - 2013-03-07 00:10)

Priority	Flows	Average flows	Bytes	Average bytes	Packets	Average packets
High priority	2.0 flows	0.3 flows	692.0 B	115.3 B	12.0 packets	2.0 packets
Medium priority	0.0 flows	0.0 flows	0.0B	0.0B	0.0 packets	0.0 packets
Low priority	1.6 k flows	263.0 flows	6.8 GiB	1.1 GiB	9.2 M packets	1.5 M packets
Legitimate traffic	16.3 k flows	2.7 k flows	294.1 MiB	49.0 MiB	438.3 k packets	73.0 k packets
Total traffic	17.9 k flows	3.0 k flows	7.1 GiB	1.2 GiB	9.7 M packets	1.6 M packets

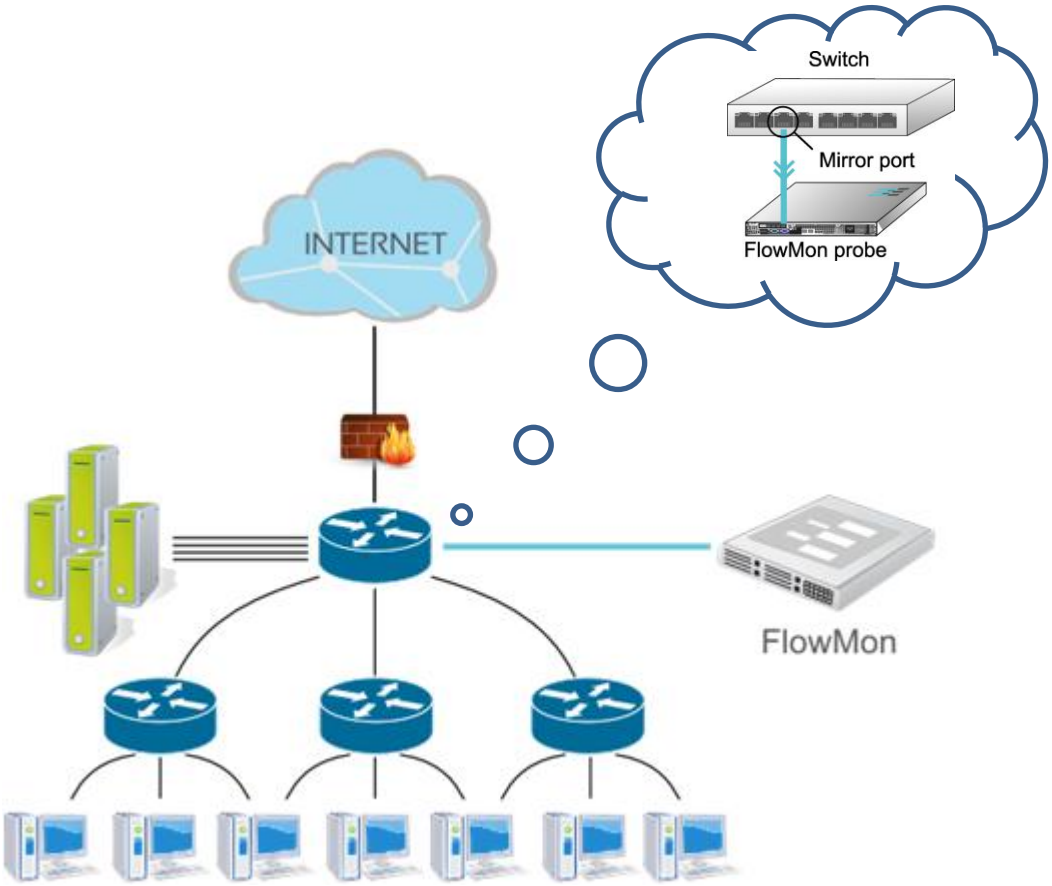
Top 10 events by priority (2013-03-06 23:40 - 2013-03-07 00:10)

#	Priority	Event type	Source	Target
1	VERY HIGH	SSHDICT	85.112.114.177	192.168.3.110, ...
2	VERY HIGH	SSHDICT	85.112.114.177	192.168.3.110, ...
3	VERY HIGH	SSHDICT	85.112.114.177	192.168.3.110, ...
4	HIGH	OUTSPAM	192.168.3.110	212.96.160.170
5	HIGH	OUTSPAM	192.168.3.169	212.96.160.170
6	HIGH	OUTSPAM	192.168.3.110	212.96.160.170
7	HIGH	OUTSPAM	192.168.3.169	212.96.160.170
8	LOW	MULTICAST	fe80::a139:5cfa:ac98:8217	ff02::16, ...
9	LOW	MULTICAST	fe80::1dea:e76b:f3d2:f069	ff02::2, ...
10	LOW	MULTICAST	fe80::b102:e114:28d2:fff0	ff02::c, ...



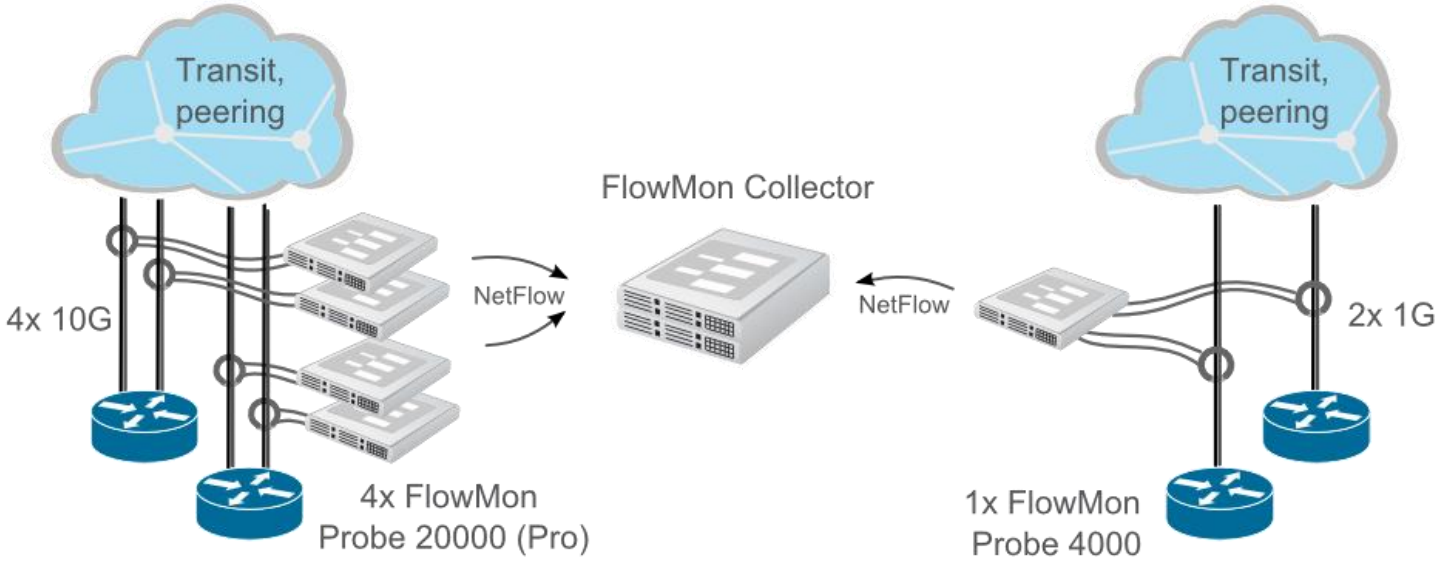
Typické nasazení – enterprise

- Sondy v jednotlivých lokalitách, centrální kolektory
- Monitorování provozu
  - Klienti – servery
  - Klienti – WAN
  - Servery – WAN
- Výstupy
  - Webové rozhraní
  - E-mailové alerty
  - SIEM (syslog)



Typické nasazení – ISP

- Sondy na jednotlivých up-linkách – NIX, zahraniční tranzit
- Monitorování provozu
  - Všechny IP obsluhované daným ISP



FlowMon shrnutí

Srovnání s tradičním přístupem

	Tradiční metody a přístupy	FlowMon
Místo instalace	Perimetr	LAN, datové centrum, perimetr
Metoda detekce	Analýza L7, na základě signatur	Analýza L3/L4, statistika, chování
Druh hrozeb	Známé hrozby	Známé L3/L4 a neznámé hrozby
Rozsah	Bezpečnostní hrozby	Bezpečnostní, provozní a výkonnostní problémy

- Cílem řešen FlowMon je doplnit a rozšířit schopnosti tradičních nástrojů pro ochranu sítě a detekci anomálií!

INVEA-TECH

- Česká společnost, univerzitní spin-off, spolupráce CESNET a univerzity, projekty EU
- Založena 2007
- Oblasti působení:
  - **Flow Monitoring**
  - **Network Behavior Analysis**

- Přes 200 instalací **řešení FlowMon** na českém trhu
- Vybrané reference: