

# FlowMon

 **Vaša sieť pod kontrolou!**



## FlowMon

- Profesionálne meranie a analýza sieťovej prevádzky
- Prináša kompletný pohľad na sieťovú prevádzku a jej štruktúru, čo sú kritické informácie pre každého správcu siete, riaditeľa IT a manažéra
- Zamerané na bezpečnosť a konfiguračné problémy
- Zahŕňa analýzu výkonnosti a sieťových kapacít
- Používa najmodernejšie metódy a nástroje
- Analýza sa vykonáva s použitím FlowMon sondy
- Výstupom služby je dokument detailnej analýzy
- Súčasťou služby je zápožička FlowMon sondy



# FlowMon

## NTA - Vzorová analýza



**Type: SSH Dictionary Attacks (SSHDICT)**  
 Timestamp: 2013-01-30 12:18:27  
 Event source host: 117.79.91.214  
 NetFlow source: demo.jivea.cz  
 Details: End of attack (unsuccessful), summary: Total count of targets: 1, maximum transferred: 1.16 KiB, total count of attempts: 22, duration of attack: 983.74 seconds. Single attack.

**Count of flows due to Transferred**

Size	Count
599 B	1
2.1 KiB	23
1.2 KiB	2
2.2 KiB	1
2.3 KiB	25

**Flows**  
**Bytes**  
**Packets**

**InveaTECH**

**V jednom prípade došlo k nahraniu veľkého objemu dát z interní sítě do sítě internet. Stanice 10.1.1.84 nahrála během dvaceti minut téměř 1GB dat na externí úložiště provozované v rámci portálu Yahoo. Domníváme se, že v tomto případě mohlo dojít k úniku dat z organizace.**  
 Analýza síťového provozu ve společnosti XYZNet  
 25.1.2013

**Mimo tuto událost bylo dále zaznamenáno ojedinělé využívání služby Dropbox stanicí 192.168.3.101. Celkem bylo přeneseno 30 MB dat. Doporučujeme ověřit, zda je využívání služby Dropbox legitimní.**

**P2P sítě**  
 Na stanici 192.168.201.120 byl detekován aktivní klient P2P sítě Bittorrent. Toto chování trvalo po celou dobu monitoringu. Uživatel stanici zřejmě využívá ke stahování obsahu prostřednictvím P2P sítě. Na časové ose níže jsou barevně vyznačeny časové úseky, kdy bylo používání klienta Bittorrent detekováno. Vzhledem k celkovému 359 počtu událostí se jedná o masivní soustavnou aktivitu uživatele. Následuje vypis několika zaznamenaných událostí.

**Infikované stanice**  
 V průběhu sledované sítě XYZNet byly detekovány kontakty externí sítě. Z níže uvedeného seznamu doporučujeme zkontrolovat infikované stanice.

**09:55 došlo ke zvýšení počtu komunikací mezi mail.abcd.cz:imaps). Bylo vytvořeno přes 277 tisíc paketů a přeneseno cca. 33,5 MB dat. Zřejmě se jedná o výpadek serveru, který se reagovala opakovanými pokusy o připojení ke službě.**

Start Time	First seen	Duration	Protocol	Source IP address	Source Port	Destination IP address	Destination Port	TCP Flags	Input Src Addr	Output Dest Addr	Sys. I/O MB	31% I/O	Packets	Bytes	Packets per second	Bits per second	Bytes per packet	Flow
2013-08-22 08:40:36.001	8.000	TCP	192.168.4.130	5876	123.34.56.78	80	...	...	00:0c:29:c0:c0:28	00:1e:a7:05:ab:30	3	0	1	52	0	0	52	1
2013-08-22 08:40:36.000	2.989	TCP	192.168.4.130	5887	123.34.56.78	80	...	...	00:0c:29:c0:c0:28	00:1e:a7:05:ab:30	3	0	4	208	1	505	52	1
2013-08-22 08:40:37.000	8.000	TCP	192.168.4.130	5888	123.34.56.78	80	...	...	00:0c:29:c0:c0:28	00:1e:a7:05:ab:30	3	0	1	52	0	0	52	1
2013-08-22 08:40:36.999	2.999	TCP	192.168.4.130	5889	123.34.56.78	80	...	...	00:0c:29:c0:c0:28	00:1e:a7:05:ab:30	3	0	4	208	1	504	52	1
2013-08-22 08:41:39.497	11.026	TCP	192.168.4.130	5870	123.34.56.78	80	...	...	00:0c:29:c0:c0:28	00:1e:a7:05:ab:30	3	0	4	216	0	126	54	1