Network Traffic Monitoring & Security

from academic project to commercial product

INVEATECH

GÉANT

Petr Špringl
springl@invea.com

Campus network monitoring
and security workshop, 24.4.2014

Agenda

- INVEA-TECH Introduction
    - from academic project to commercial company
- FlowMon Solution Introduction
- Typical Use Cases from Corporate Environments
- FlowMon for R&D purposes

Company Introduction

- Czech university spin-off company
- Established in 2007
- 40+ employees, $ 3M revenue
- Key focus
  - **Flow Monitoring and Network Behavior Analysis**
  - **Hardware acceleration and FPGA Solutions**

- Products deployed at 500+ customers worldwide

vmware PARTNER TECHNOLOGY ALLIANCE

CISCO DEVELOPER Registered

Gartner Research

ID Number: G00208386

CERTIFICATE OF Deloitte. ACHIEVEMENT

How it began...

- CESNET started activities with programmable hardware in 2002 - project Liberouter
- Cooperation with Masaryk University and Brno University of Technology
- Targets:
  - acceleration of high-speed network application (IPv6 router)
  - usage of programmable hardware
  - development of hardware accelerators COMBO based on FPGA technology for acceleration of critical tasks in data processing
- Participation on EU project 6NET (IST-2001-32063)
- Continuous growth and formation of strong R&D team in area of programmable hardware and high-speed network application

…continues…

- Successful end of 6NET project
- Cooperation on next EU projects
- SCAMPI (IST-2001-32404)
  - 2002 – 2005, network monitoring of 10Gbps lines
  - joining to project in 2003 instead of commercial partners
  - functional prototype developed, successful review
  - recommendation – commercialize outputs in practice
- GEÁNT2 (contract No. 511082)
  - cooperation of 26 NRENs from 34 countries
  - activity JRA2 – focus on network security
  - functional prototype of HW accelerated NetFlow probe - FlowMon
  - final recommendation – monitor network by the NetFlow probe
  - GEÁNT2 Security Toolset – FlowMon Probes & NfSen collector

…ended, and began

- June 2007 – INVEA-TECH was established
- Technology transfer from CESNET to INVEA-TECH
  - hard to find right model
  - first technology transfer from CESNET

UNIVERSITAS MASARYKIANA BRUNENSIS

- INVEA-TECH
  - long way from prototype to product
  - close cooperation with academic area (CESNET, Czech and abroad universities, EU projects)

Products Portfolio

- FPGA products
  - COMBO cards
  - NetCOPE platform
  - High-speed appliances

- FlowMon solution
  - Network traffic monitoring and security solution
  - Flagship product

FlowMon Solution

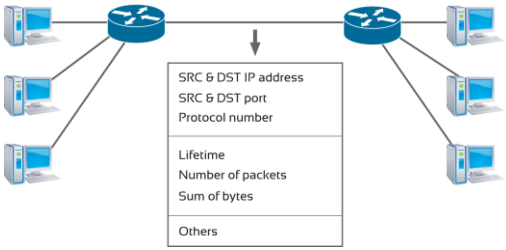
- Network Traffic Monitoring and Security solution

- **DETAILED NETWORK TRAFFIC VISIBILITY**
  - Do you know what's really happening in your network – not only to Internet but also in LAN and WAN? Real-time and historically?
  - Are you paying too much for Internet or WAN connection?
  - Is your network slow?

- **ANOMALY DETECTION** (based on Network Behavior Analysis - NBA)
  - Do you easily detect DOS/DDOS, and attacks against services?
  - What about APTs, zero-day attacks and polymorphic malware?
  - Are you able to reveal viruses/malware not detected by antivirus?

FlowMon Solution

- Based on **IP flows monitoring** (**NetFlow** v5/v9 and **IPFIX** technology)
- Provides information about **who** communicates with **whom**, **how long**, **what protocol**, **traffic volume** and more
- **Network Behavior Analysis** (NBA) detects network anomalies, suspicious behavior, changes in behavior and any suspicious communication

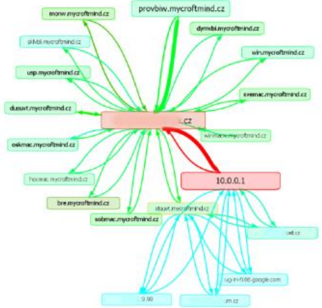


SRC & DST IP address
SRC & DST port
Protocol number

Lifetime
Number of packets
Sum of bytes

Others

```
Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags
   2.096 TCP               56956 ->       108.7.1.50:80     .AP.S.
   0.094 TCP         108.7.1.5   ->    59.173.182.61:49442  .AP.S.
   0.368 TCP         108.7.1.50  ->    59.173.182.61:49440  .AP.S.
   0.737 TCP                     ->    59.173.182.61:49434  .AP.S.
   0.379 TCP         108.7.1.50: ->    59.173.182.61:49438  .AP.S.
   0.296 TCP                     ->       108.7.1.50:80     .AP.S.
   0.575 TCP      59.173.182.61:4 ->      108.7.1.50:80     .AP.S.
   0.574 TCP      59.173.182.61: ->       108.7.1.50:80     .AP.S.
   0.451 TCP                     ->       108.7.1.50:80     .AP...
   1.281 TCP      59.173.182.61: ->       108.7.1.50:80     .AP.SF
   1.280 TCP                            .233.173:41667      .AP.SF
   5.886 TCP      59.173.182.6   ->          .129:1687      .AP...
   6.051 TCP        13.233    687 ->             50:80      .AP...
   2.800 TCP                 :80 ->    210.          607    .AP.S.
   2.980 TCP   210.56.6.116:56607 ->      108.7.            AP.S.
   1.693 TCP        108.7.1.50:80 -> 157.242.141.1
   1.778 TCP        108.7.1.50:80 -> 157.242.141.183:13
   0.604 TCP 157.242.141.183:1325 ->      108.7.1.50:80
   1.990 TCP 157.242.141.183:1324 ->      108.7.1.50:80     .AP.S.
```

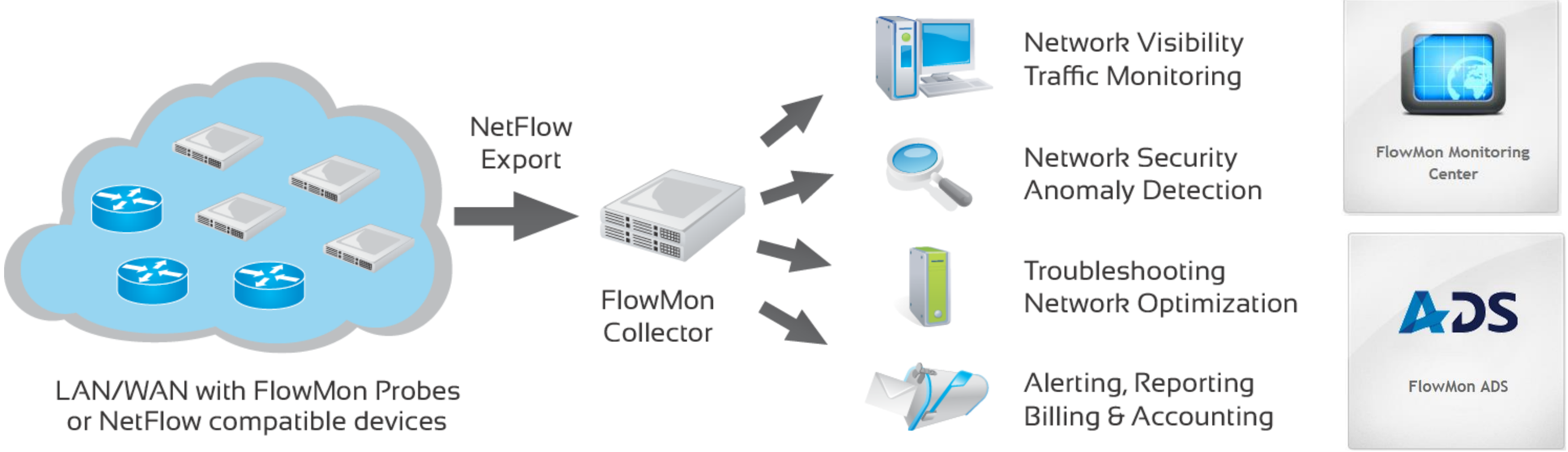


FlowMon Architecture

INVEATECH

- FlowMon Probes
  - source of network statistics (NetFlow, IPFIX)
- FlowMon Collectors
  - visualization and evaluation of network statistics
- FlowMon ADS
  - detection of attacks, anomalies and undesirable behavior

vmware



FlowMon Probe

- High-performance standalone probe - source of IP flow records in NetFlow v5,9 and IPFIX format
- 1U rack appliance / VMware appliance
- Leadership in performance
  - wire-speed models

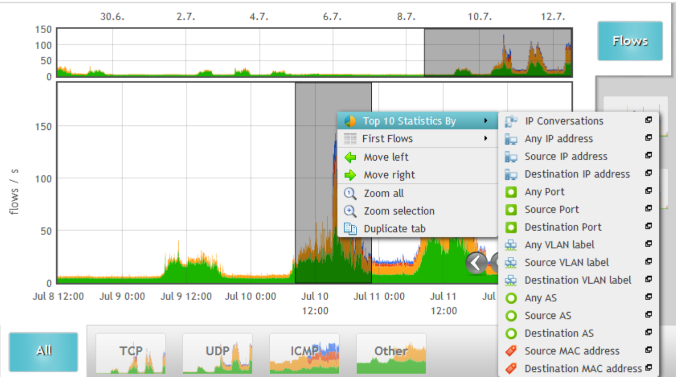
- Up to 6x 1G, 8x 10G, 2x 40G, 1x 100G monitoring interfaces
- 10MbE to 100GbE, IPv4/IPv6, MPLS, VLAN, GRE …
- Application detection (NBAR2), VoIP (SIP/RTP), URLs, network performance monitoring (ART, SRT, Delay)…

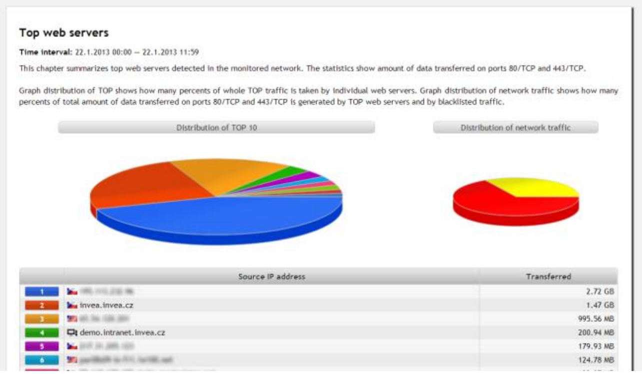
FlowMon Collector

- Appliance for flow data storage & analysis
  - 1U/2U/VMware appliance
- NetFlow v5/v9, IPFIX, sFlow, Netstream… support
- Based on nfdump/NfSen, but completely redesigned and you wouldn't recognize it
- Tuned & optimized to be suitable for the largest networks (>200k fps)

FlowMon Collector

- More user friendly, automation, optimizations
- Automatic flow data source detections
- User defined dashboard
- Improved Top N statistics
- Enhanced alerting
- Intelligent reporting - online/email, PDF/CSV
- IPFIX support, extended about lot of fields
- Fast & easy configuration
- …..





Top web servers

Time interval: 22.1.2013 00:00 – 22.1.2013 11:59

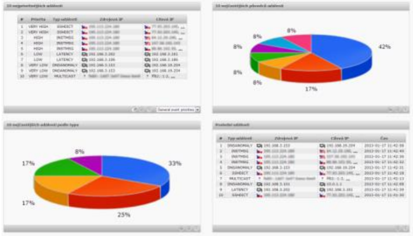
This chapter summarizes top web servers detected in the monitored network. The statistics show amount of data transferred on ports 80/TCP and 443/TCP.

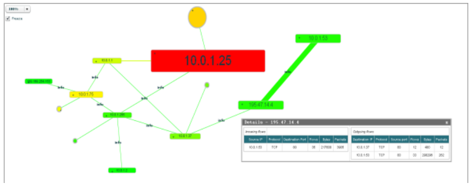
Graph distribution of TOP shows how many percents of whole TOP traffic is taken by individual web servers. Graph distribution of network traffic shows how many percents of total amount of data transferred on ports 80/TCP and 443/TCP is generated by TOP web servers and by blacklisted traffic.

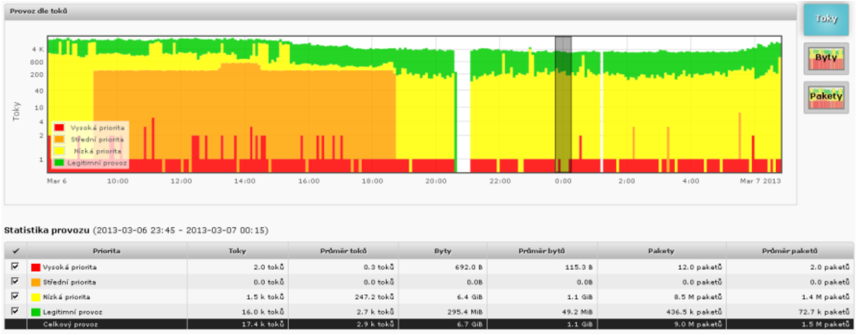
	Source IP address	Transferred
1	[redacted]	2.72 GB
2	invea.invea.cz	1.47 GB
3	[redacted]	995.56 MB
4	demo.intranet.invea.cz	200.94 MB
5	[redacted]	179.93 MB
6	[redacted]	124.78 MB

FlowMon ADS

- **System for automatic network traffic analysis**
  - Detection of security & operational incidents and suspicious behavior
- Undesirable patterns in communications
  - Internal and external attacks
  - Undesirable services & applications
  - Operational & configuration problems
- Behavior Analysis
  - Behavior profiles
  - Anomalies detection





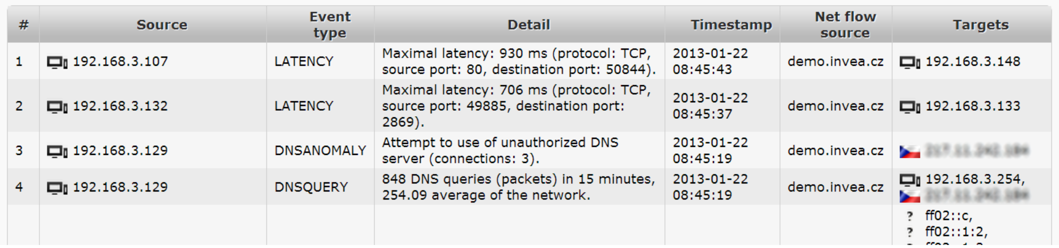


Statistika provozu (2013-03-06 23:45 - 2013-03-07 00:15)

✓	Priorita	Toky	Průměr toků	Byty	Průměr bytů	Pakety	Průměr paketů
☑	🟥 Vysoká priorita	2.0 toků	0.3 toků	692.0 B	115.3 B	12.0 paketů	2.0 paketů
☑	🟧 Střední priorita	0.0 toků	0.0 toků	0.0B	0.0B	0.0 paketů	0.0 paketů
☑	🟨 Nízká priorita	1.5 k toků	247.2 toků	6.4 GiB	1.1 GiB	8.5 M paketů	1.4 M paketů
☑	🟩 Legitimní provoz	16.0 k toků	2.7 k toků	295.4 MiB	49.2 MiB	436.5 k paketů	72.7 k paketů
	Celkový provoz	17.4 k toků	2.9 k toků	6.7 GiB	1.1 GiB	9.0 M paketů	1.5 M paketů

FlowMon ADS

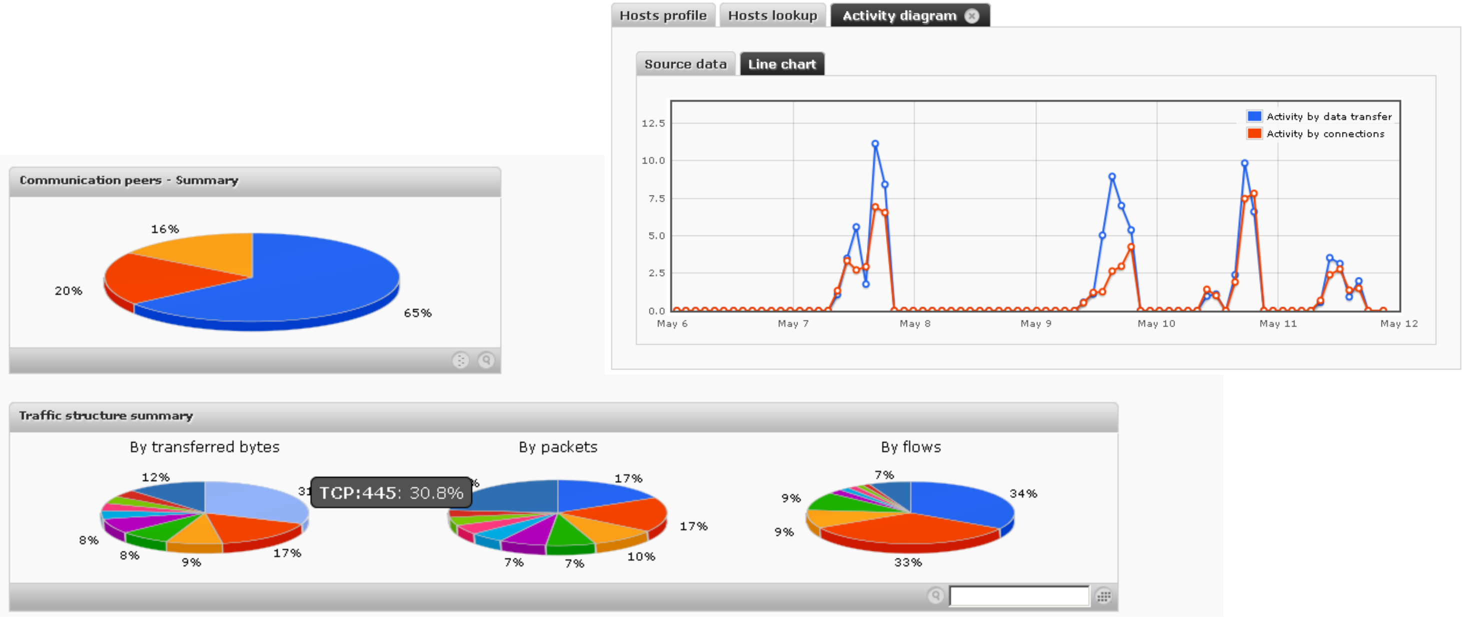
- Detection of undesirable patterns in communication
  - Attacks (port scanning, dictionary attacks, denial of service, telnet protocol)
  - Data traffic anomalies (DNS, multicast, non-standard communications)
  - Device behavior anomalies (changes in long-term device behavior profile)
  - Undesirable applications (P2P networks, instant messenger, anonymizer)
  - Internal security problems (viruses, spyware, botnets)
  - Mail traffic (outgoing spam)
  - Operational problem (delays, high traffic, reverse DNS records)



#	Source	Event type	Detail	Timestamp	Net flow source	Targets
1	192.168.3.107	LATENCY	Maximal latency: 930 ms (protocol: TCP, source port: 80, destination port: 50844).	2013-01-22 08:45:43	demo.invea.cz	192.168.3.148
2	192.168.3.132	LATENCY	Maximal latency: 706 ms (protocol: TCP, source port: 49885, destination port: 2869).	2013-01-22 08:45:37	demo.invea.cz	192.168.3.133
3	192.168.3.129	DNSANOMALY	Attempt to use of unauthorized DNS server (connections: 3).	2013-01-22 08:45:19	demo.invea.cz	[redacted]
4	192.168.3.129	DNSQUERY	848 DNS queries (packets) in 15 minutes, 254.09 average of the network.	2013-01-22 08:45:19	demo.invea.cz	192.168.3.254, [redacted] ? ff02::c, ? ff02::1:2,

FlowMon ADS

- Behavior analysis
  - Behavior profile (client/server, data traffic, partners, traffic structure)
  - Anomaly detection (actual behavior against long-term profile)
  - Statistics information (continues indicators about network behavior)



Use Cases

Color	Start Time - first seen	Duration	Protocol	Any Port	Flows	Input Packets	Input Bytes
1	07/09/2012 - 1:09:38 PM	5m, 7s	any	993	339 (83.1%)	6.24 K (81.8%)	736.74 KB (60.8%)
2	07/09/2012 - 1:10:48 PM		any	995	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
3	07/09/2012 - 1:10:48 PM		any	51429	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
4	07/09/2012 - 1:10:39 PM	2m, 13s	any	52029	3 (0.7%)	1.66 K (21.8%)	206.88 KB (17.1%)
5	07/09/2012 - 1:10:05 PM	3m, 48s	any	58990	5 (1.2%)	141 (1.8%)	114.89 KB (9.5%)
6	07/09/2012 - 1:10:08 PM	4m, 26s	any	143	60 (14.7%)	945 (12.4%)	95.89 KB (7.9%)
7	07/09/2012 - 1:10:04 PM	4m, 6s	any	59619	10 (2.5%)	177 (2.3%)	18.54 KB (1.5%)
8	07/09/2012 - 1:10:01 PM	3m, 59s	any	59286	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
9	[illegible]	3m, 59s	any	59436	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
			any	58813	10 (2.5%)	162 (2.1%)	17.41 KB (1.4%)
				s 408		Bytes 1.18 MB	Packets 7.63 K

Analyzed traffic

Profile: live

Segment: Last 4 days

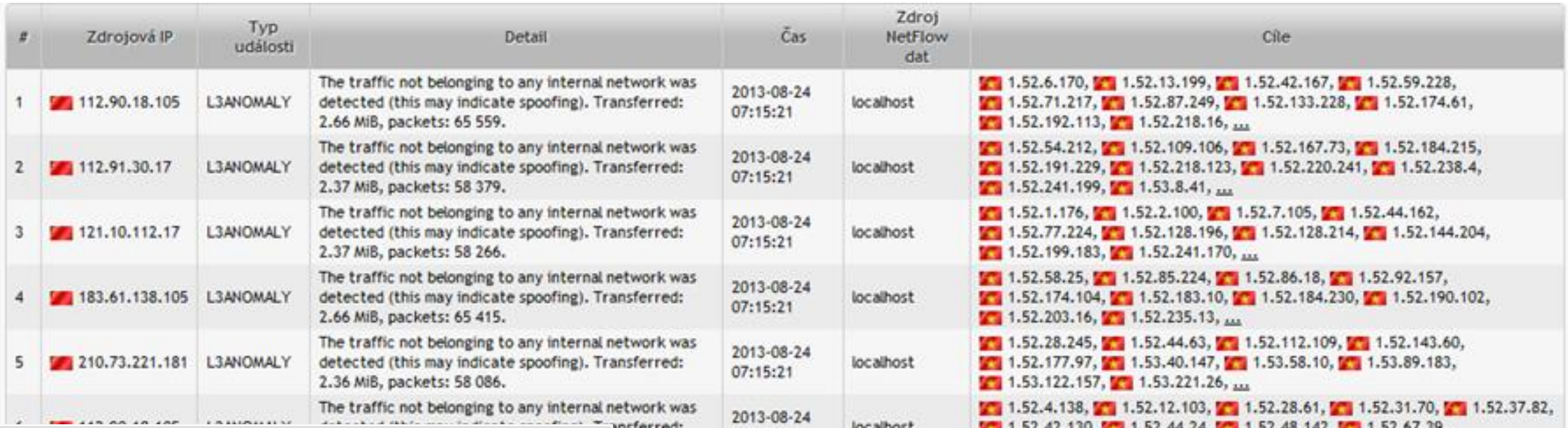
From: 08.07.2012 11:55

To: 12.07.2012 11:55

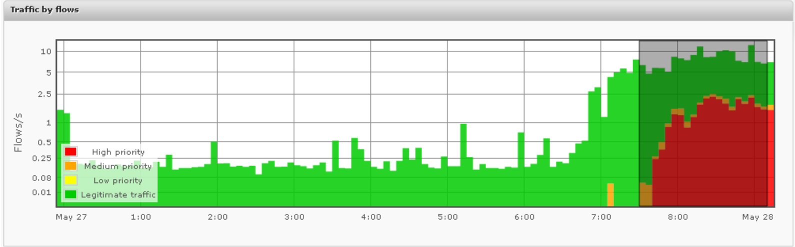
Typical real use cases from our customers

DDoS from Spoofed IPs

- Finance instituions
- Several workstations infected by botnet
- Spoofed China IPs attack to Vietnam



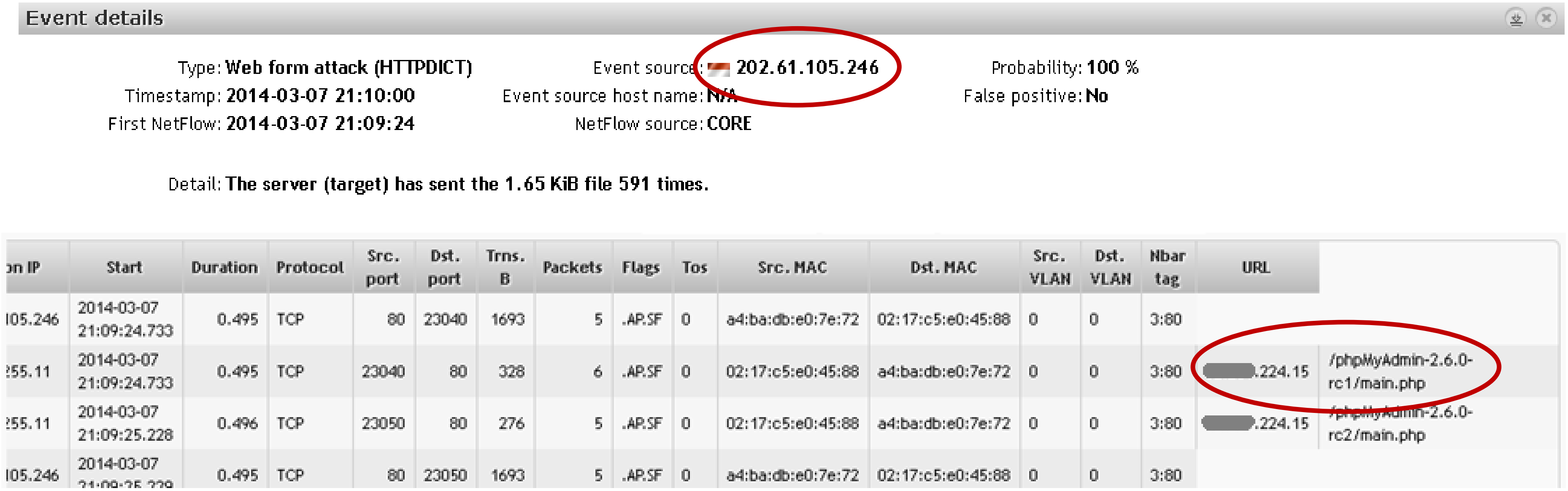
#	Zdrojová IP	Typ události	Detail	Čas	Zdroj NetFlow dat	Cíle
1	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 559.	2013-08-24 07:15:21	localhost	1.52.6.170, 1.52.13.199, 1.52.42.167, 1.52.59.228, 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.174.61, 1.52.192.113, 1.52.218.16, ...
2	112.91.30.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 379.	2013-08-24 07:15:21	localhost	1.52.54.212, 1.52.109.106, 1.52.167.73, 1.52.184.215, 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52.238.4, 1.52.241.199, 1.53.8.41, ...
3	121.10.112.17	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.37 MiB, packets: 58 266.	2013-08-24 07:15:21	localhost	1.52.1.176, 1.52.2.100, 1.52.7.105, 1.52.44.162, 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52.144.204, 1.52.199.183, 1.52.241.170, ...
4	183.61.138.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.66 MiB, packets: 65 415.	2013-08-24 07:15:21	localhost	1.52.58.25, 1.52.85.224, 1.52.86.18, 1.52.92.157, 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52.190.102, 1.52.203.16, 1.52.235.13, ...
5	210.73.221.181	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.36 MiB, packets: 58 086.	2013-08-24 07:15:21	localhost	1.52.28.245, 1.52.44.63, 1.52.112.109, 1.52.143.60, 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89.183, 1.53.122.157, 1.53.221.26, ...
6	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred:	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.70, 1.52.37.82, 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67.39, 1.52.83.34, ...
			etwork was ansferred:	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.90, 1.52.74.20, 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.119.156, 1.52.122.10, ...
			etwork was ansferred:	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125.205, 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52.139.229, 1.52.203.143, 1.52.209.197, ...
			etwork was			1.52.32.201, 1.52.44.55, 1.52.87.138, 1.52.122.97



Traffic by flows

Authentication Attack

- Healthcare
- Attacker IP somewhere from Indonesia
- Attacks against phpMyAdmin web application
- Exposed to public Internet but not necessary



Event details

Type: **Web form attack (HTTPDICT)**
Timestamp: **2014-03-07 21:10:00**
First NetFlow: **2014-03-07 21:09:24**

Event source: **202.61.105.246**
Event source host name: **N/A**
NetFlow source: **CORE**

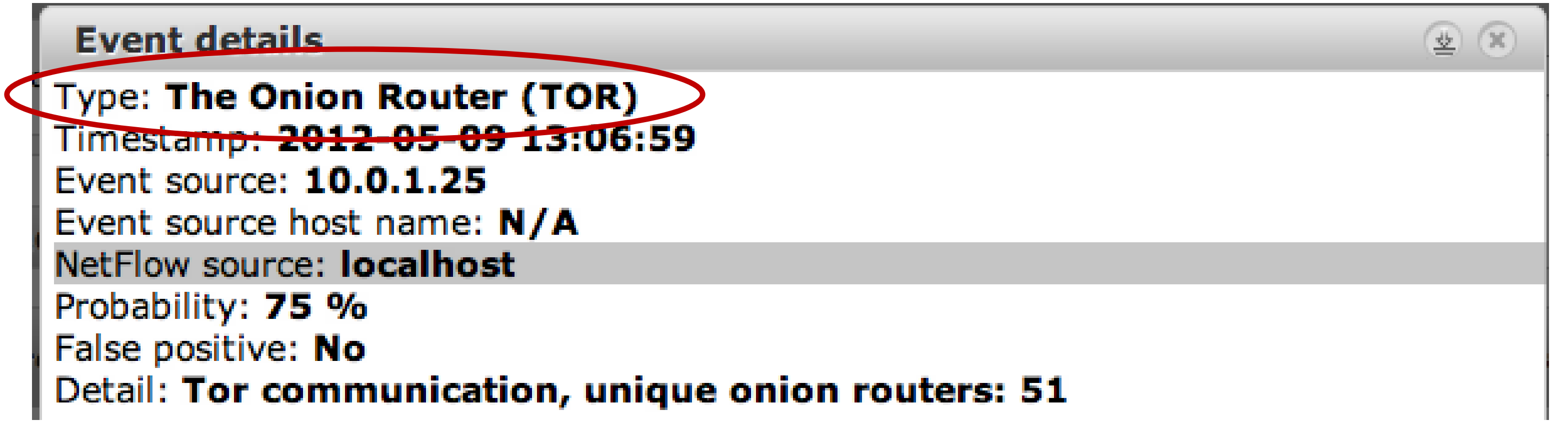
Probability: **100 %**
False positive: **No**

Detail: **The server (target) has sent the 1.65 KiB file 591 times.**

on IP	Start	Duration	Protocol	Src. port	Dst. port	Trns. B	Packets	Flags	Tos	Src. MAC	Dst. MAC	Src. VLAN	Dst. VLAN	Nbar tag	URL	
105.246	2014-03-07 21:09:24.733	0.495	TCP	80	23040	1693	5	.AP.SF	0	a4:ba:db:e0:7e:72	02:17:c5:e0:45:88	0	0	3:80		
255.11	2014-03-07 21:09:24.733	0.495	TCP	23040	80	328	6	.AP.SF	0	02:17:c5:e0:45:88	a4:ba:db:e0:7e:72	0	0	3:80	[redacted].224.15	/phpMyAdmin-2.6.0-rc1/main.php
255.11	2014-03-07 21:09:25.228	0.496	TCP	23050	80	276	5	.AP.SF	0	02:17:c5:e0:45:88	a4:ba:db:e0:7e:72	0	0	3:80	[redacted].224.15	/phpMyAdmin-2.6.0-rc2/main.php
105.246	2014-03-07 21:09:25.229	0.495	TCP	80	23050	1693	5	.AP.SF	0	a4:ba:db:e0:7e:72	02:17:c5:e0:45:88	0	0	3:80		

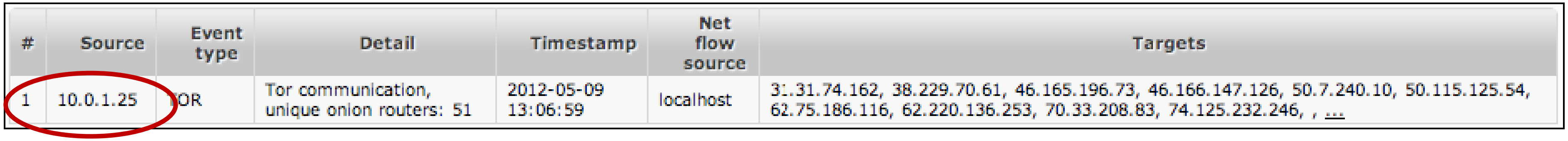
Policy violations

- Manufacturing
- TOR (Onion router) client on laptop
- Use is bypassing security measures
  - To access resources blocked by company policy



Event details

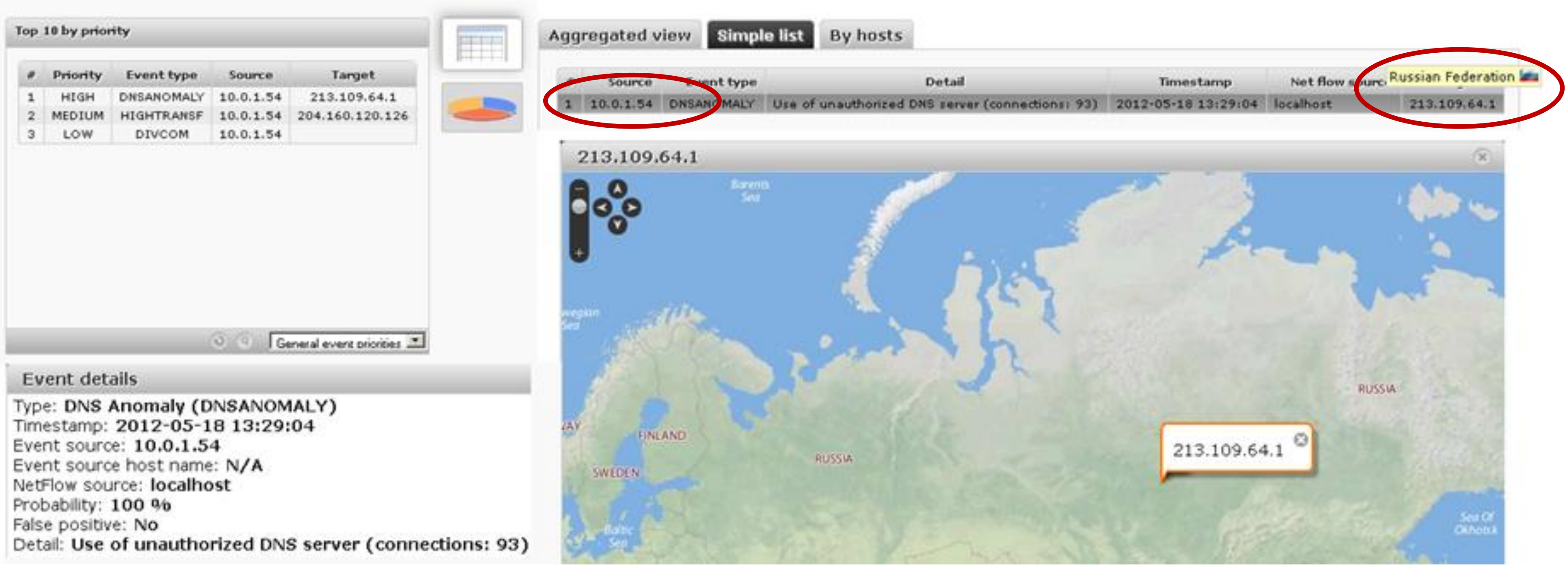
Type: **The Onion Router (TOR)**
Timestamp: **2012-05-09 13:06:59**
Event source: **10.0.1.25**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **75 %**
False positive: **No**
Detail: **Tor communication, unique onion routers: 51**



#	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	31.31.74.162, 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, , ...

DNS Changer

- Information technology
- Change of DNS server that is being used
- Attacker can manipulate with DNS records and redirect the user to malicious or phishing sites



Top 10 by priority

#	Priority	Event type	Source	Target
1	HIGH	DNSANOMALY	10.0.1.54	213.109.64.1
2	MEDIUM	HIGHTRANSF	10.0.1.54	204.160.120.126
3	LOW	DIVCOM	10.0.1.54	

Event details

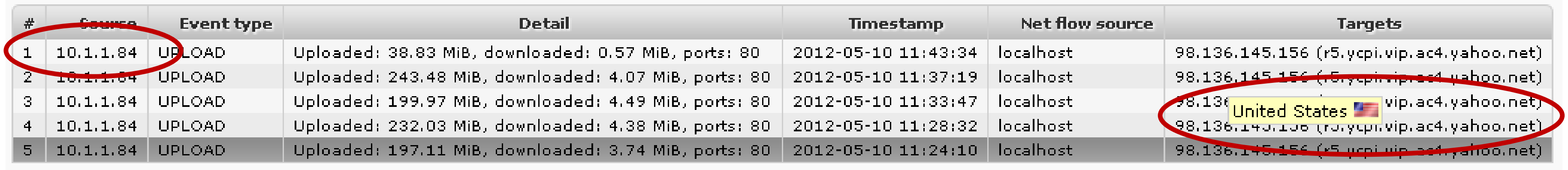
Type: **DNS Anomaly (DNSANOMALY)**
Timestamp: **2012-05-18 13:29:04**
Event source: **10.0.1.54**
Event source host name: **N/A**
NetFlow source: **localhost**
Probability: **100 %**
False positive: **No**
Detail: **Use of unauthorized DNS server (connections: 93)**

#	Source	Event type	Detail	Timestamp	Net flow source	Russian Federation
1	10.0.1.54	DNSANOMALY	Use of unauthorized DNS server (connections: 93)	2012-05-18 13:29:04	localhost	213.109.64.1

213.109.64.1

Data Leakage

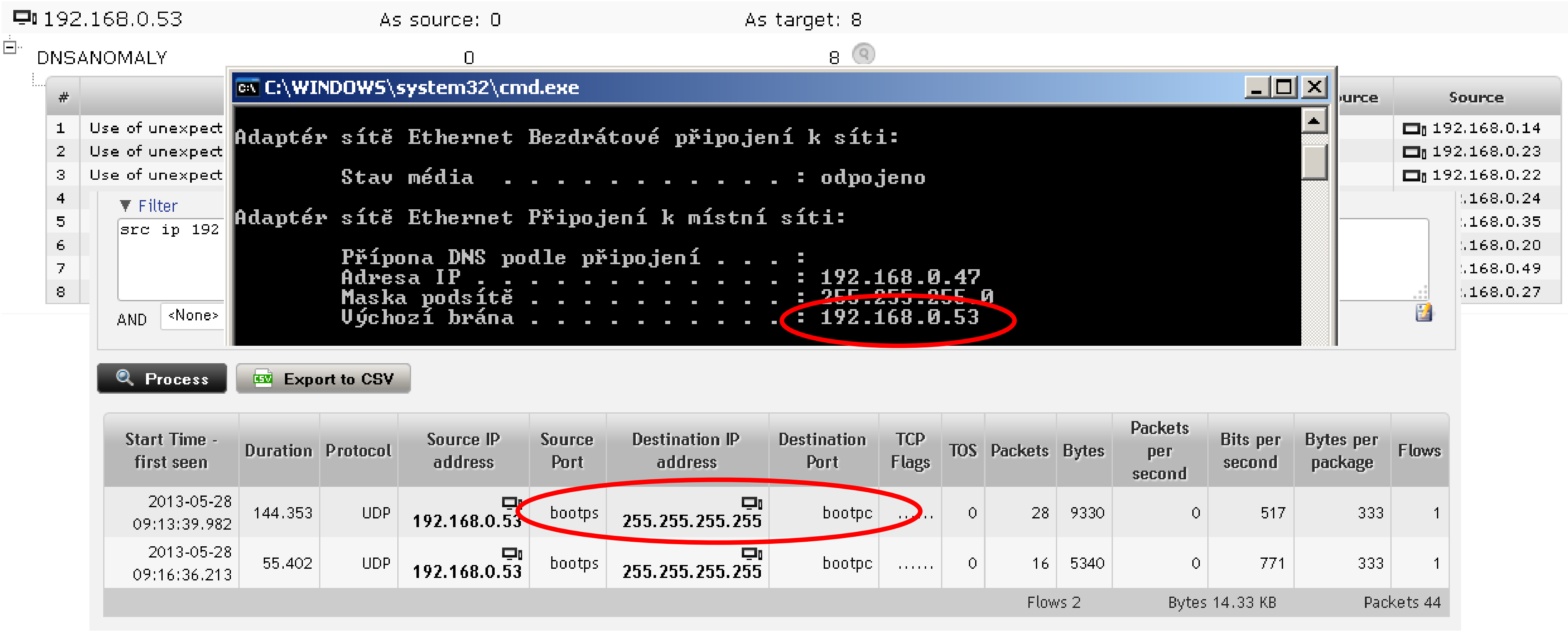
- Retail
- Employee leaving the company
- Internal documents were stored on public data share service hosted by Yahoo
- Detected as data upload from LAN to the Internet
- Inspected and evaluated as serious issue



#	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	98.136 [illegible] 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)

Sniffing of Network Traffic

- Services
- Malware use DHCP spoofing to introduce itself as gateway and to sniff the traffic



192.168.0.53 As source: 0 As target: 8

DNSANOMALY 0 8

#		Source
1	Use of unexpect	192.168.0.14
2	Use of unexpect	192.168.0.23
3	Use of unexpect	192.168.0.22
4		.168.0.24
5		.168.0.35
6		.168.0.20
7		.168.0.49
8		.168.0.27

Filter

src ip 192

AND <None>

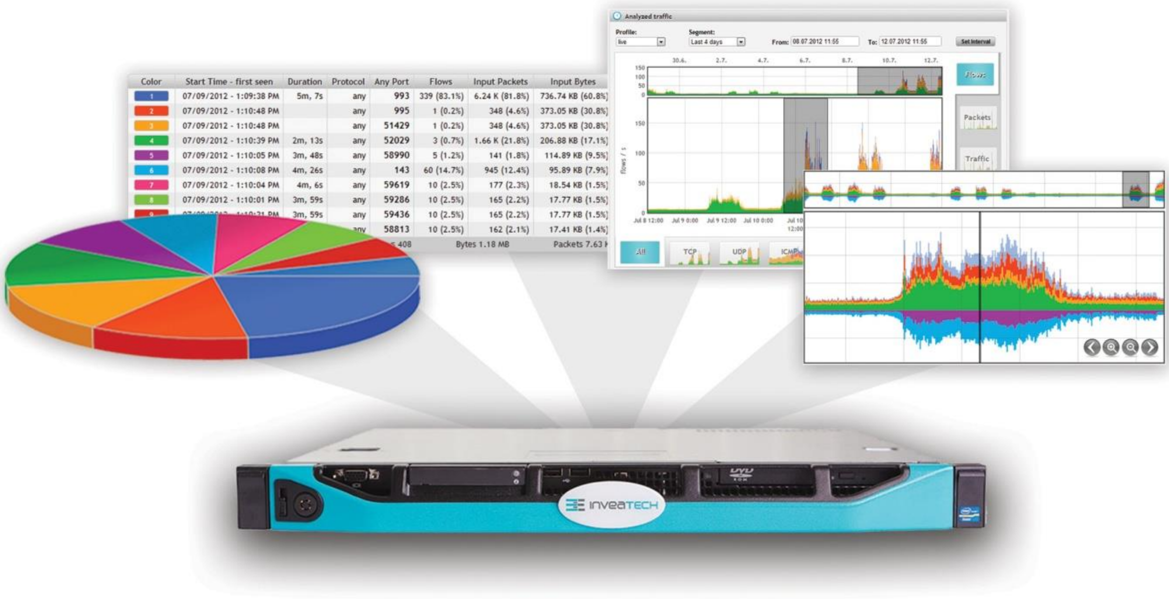
C:\WINDOWS\system32\cmd.exe

```
Adaptér sítě Ethernet Bezdrátové připojení k síti:

        Stav média  . . . . . . . . . . . : odpojeno

Adaptér sítě Ethernet Připojení k místní síti:

        Přípona DNS podle připojení . . . :
        Adresa IP . . . . . . . . . . . . : 192.168.0.47
        Maska podsítě . . . . . . . . . . : 255.255.255.0
        Výchozí brána . . . . . . . . . . : 192.168.0.53
```

Start Time - first seen	Duration	Protocol	Source IP address	Source Port	Destination IP address	Destination Port	TCP Flags	TOS	Packets	Bytes	Packets per second	Bits per second	Bytes per package	Flows
2013-05-28 09:13:39.982	144.353	UDP	192.168.0.53	bootps	255.255.255.255	bootpc	......	0	28	9330	0	517	333	1
2013-05-28 09:16:36.213	55.402	UDP	192.168.0.53	bootps	255.255.255.255	bootpc	......	0	16	5340	0	771	333	1

Flows 2 Bytes 14.33 KB Packets 44

R&D Cooperation



Color	Start Time - first seen	Duration	Protocol	Any Port	Flows	Input Packets	Input Bytes
1	07/09/2012 - 1:09:38 PM	5m, 7s	any	993	339 (83.1%)	6.24 K (81.8%)	736.74 KB (60.8%)
2	07/09/2012 - 1:10:48 PM		any	995	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
3	07/09/2012 - 1:10:48 PM		any	51429	1 (0.2%)	348 (4.6%)	373.05 KB (30.8%)
4	07/09/2012 - 1:10:39 PM	2m, 13s	any	52029	3 (0.7%)	1.66 K (21.8%)	206.88 KB (17.1%)
5	07/09/2012 - 1:10:05 PM	3m, 48s	any	58990	5 (1.2%)	141 (1.8%)	114.89 KB (9.5%)
6	07/09/2012 - 1:10:08 PM	4m, 26s	any	143	60 (14.7%)	945 (12.4%)	95.89 KB (7.9%)
7	07/09/2012 - 1:10:04 PM	4m, 6s	any	59619	10 (2.5%)	177 (2.3%)	18.54 KB (1.5%)
8	07/09/2012 - 1:10:01 PM	3m, 59s	any	59286	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
9	07/09/2012 - 1:10:21 PM	3m, 59s	any	59436	10 (2.5%)	165 (2.2%)	17.77 KB (1.5%)
			any	58813	10 (2.5%)	162 (2.1%)	17.41 KB (1.4%)
				s 408		Bytes 1.18 MB	Packets 7.63 K

Analyzed traffic

Profile: live

Segment: Last 4 days

From: 08.07.2012 11:55

To: 12.07.2012 11:55

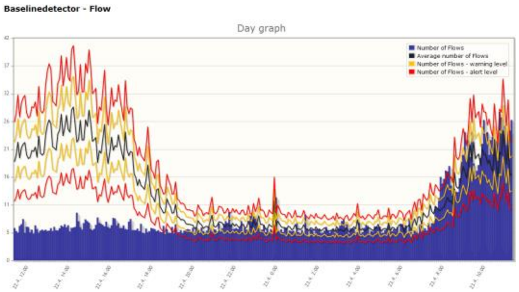
FlowMon Community program

FlowMon – Community Program

- Target
  - Enable users to make program changes to FlowMon solution
  - Don't provide closed NetFlow based solution, but rather provide possibilities to use it for further R&D in area of traffic monitoring, customize according to needs
- Open to any applicant
  - Just ask for joining and get update package to FlowMon appliance (open the API)
- Main benefits
  - Join to community around FlowMon solution
  - Access to all plugins developed in the Community program
  - Knowledge base, share experience, discussions...

FlowMon – Community Program

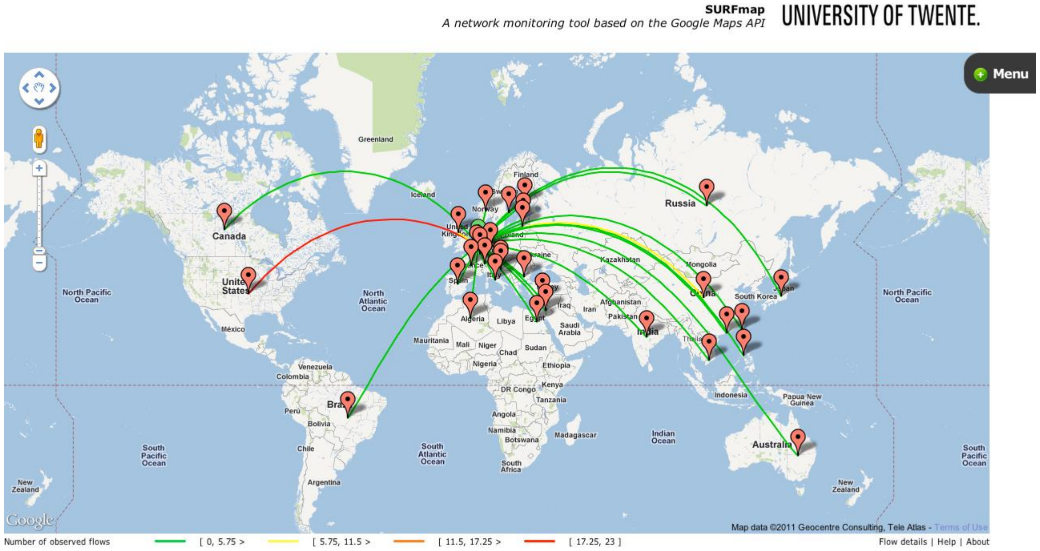
- Customization of FlowMon Probe
  - FlowMon exporter provide API for users plugins which can directly influence process of monitoring, generation and export of flow data
    - ❑ packets parsing, processing and storing to internal structures
    - ❑ computations over the flow data
    - ❑ data storing and export to collector



- Customization of FlowMon Collector
  - realized through plugins to NfSen application
  - usage of NfSen API

FlowMon - Community Program

- **University of Twente**
  - SURFmap plugin (http://sourceforge.net/p/surfmap/home/Home/)
  - Collector plugin
  - Adds a geographical dimension to network traffic
  - Based on the Google Maps API



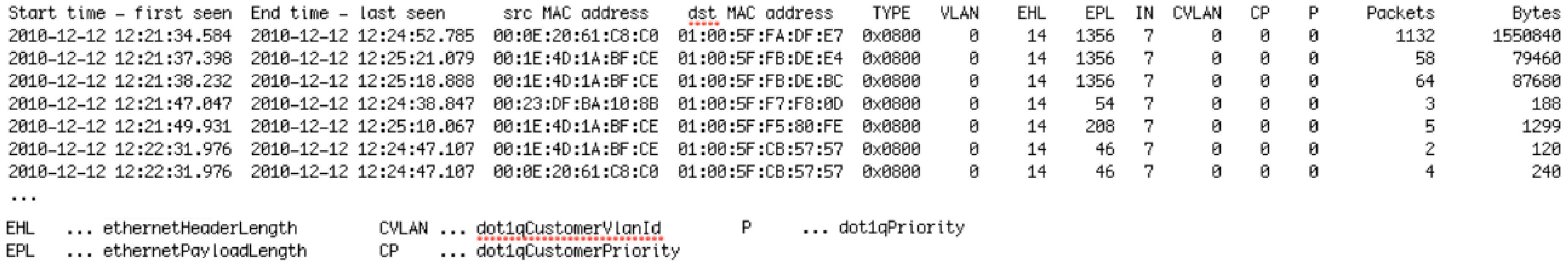
SURFmap
A network monitoring tool based on the Google Maps API
UNIVERSITY OF TWENTE.

Number of observed flows 🟩 [0, 5.75 > 🟨 [5.75, 11.5 > 🟧 [11.5, 17.25 > 🟥 [17.25, 23]

Flow details | Help | About

FlowMon - Community Program

- **University of Twente** for **SURFnet**
  - Monitoring Ethernet Networks Using IPFIX
  - Probe plugin
  - Probes monitor traffic at Ethernet-layer and use a modified process of flow creation
    - key-fields - SRC and DST MAC, VLAN ID and Ethernet type
  - Provide an overview of all traffic protocols operating on top of Ethernet (ARP, LLDP, STP, Novell IPX, ...)



```
Start time - first seen  End time - last seen     src MAC address    dst MAC address    TYPE    VLAN    EHL    EPL  IN  CVLAN   CP    P    Packets       Bytes
2010-12-12 12:21:34.584  2010-12-12 12:24:52.785  00:0E:20:61:C8:C0  01:00:5F:FA:DF:E7  0x0800     0     14   1356   7      0    0    0       1132     1550840
2010-12-12 12:21:37.398  2010-12-12 12:25:21.079  00:1E:4D:1A:BF:CE  01:00:5F:FB:DE:E4  0x0800     0     14   1356   7      0    0    0         58       79460
2010-12-12 12:21:38.232  2010-12-12 12:25:18.888  00:1E:4D:1A:BF:CE  01:00:5F:FB:DE:BC  0x0800     0     14   1356   7      0    0    0         64       87680
2010-12-12 12:21:47.047  2010-12-12 12:24:38.847  00:23:DF:BA:10:8B  01:00:5F:F7:F8:0D  0x0800     0     14     54   7      0    0    0          3         188
2010-12-12 12:21:49.931  2010-12-12 12:25:10.067  00:1E:4D:1A:BF:CE  01:00:5F:F5:80:FE  0x0800     0     14    208   7      0    0    0          5        1299
2010-12-12 12:22:31.976  2010-12-12 12:24:47.107  00:1E:4D:1A:BF:CE  01:00:5F:CB:57:57  0x0800     0     14     46   7      0    0    0          2         120
2010-12-12 12:22:31.976  2010-12-12 12:24:47.107  00:0E:20:61:C8:C0  01:00:5F:CB:57:57  0x0800     0     14     46   7      0    0    0          4         240
...

EHL   ... ethernetHeaderLength        CVLAN ... dot1qCustomerVlanId        P     ... dot1qPriority
EPL   ... ethernetPayloadLength       CP    ... dot1qCustomerPriority
```

Summary

- FlowMon solution provides data flow monitoring
  - Network operational monitoring
  - Network security monitoring
- Suitable even for the largest networks
- Can be used for further R&D in area of flow monitoring and security

High-Speed Networking Technology Partner

Petr Špringl
springl@invea.com
+420 724 899 760

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com