Network Security Monitoring with Flow Data

Anomaly Detection & DDoS Protection

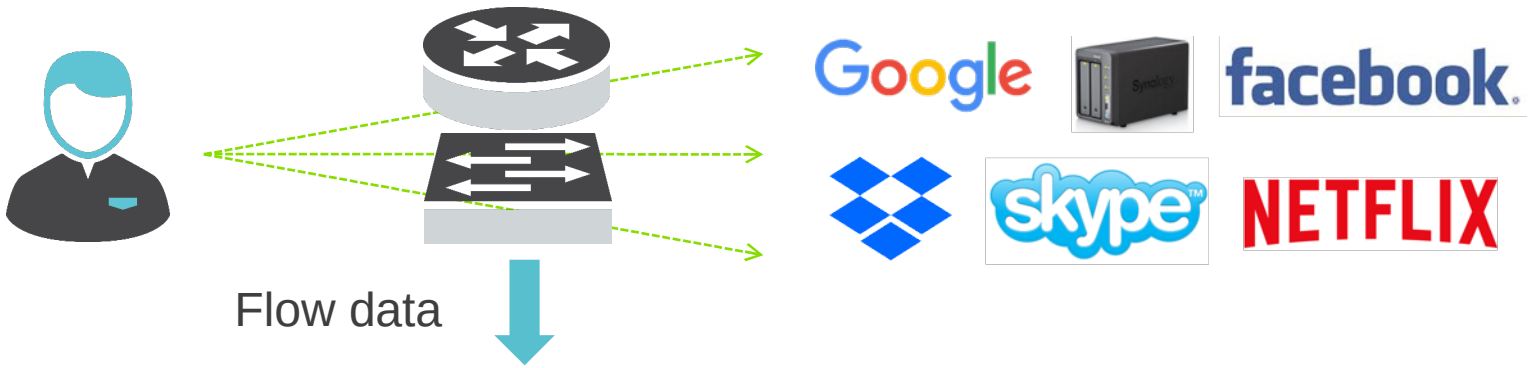
Pavel Minařík, Chief Technology Officer

Flowmon

Driving Network Visibility

What is Flow Data?

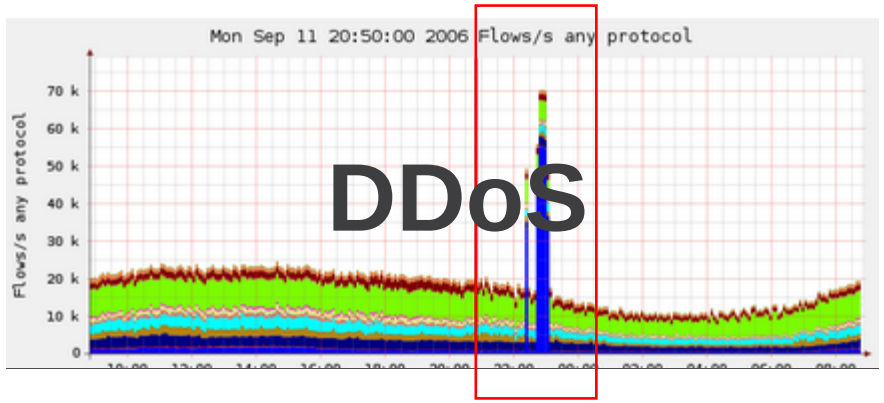
- Modern network telemetry data, supported by many vendors
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Focused on L3/L4 information and volumetric parameters
- Real network traffic to flow statistics reduction ratio 500:1



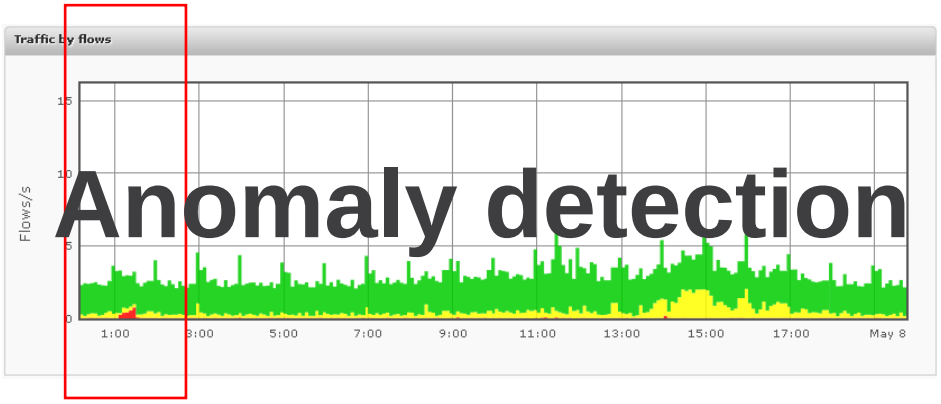
Flowmon
Driving Network Visibility

Flow-Based Traffic Analysis

- Network as a sensor concept (and enforcer)
  - blogs.cisco.com/enterprise/the-network-as-a-security-sensor-and-enforcer
- Bridges the gap left by signature-based security
- Key technology for incident response
- Designed for multi 10G environment



Statistical analysis
Volumetric DDoS detection



Advanced data analysis algorithms
Detection of non-volumetric anomalies

Flowmon
Driving Network Visibility

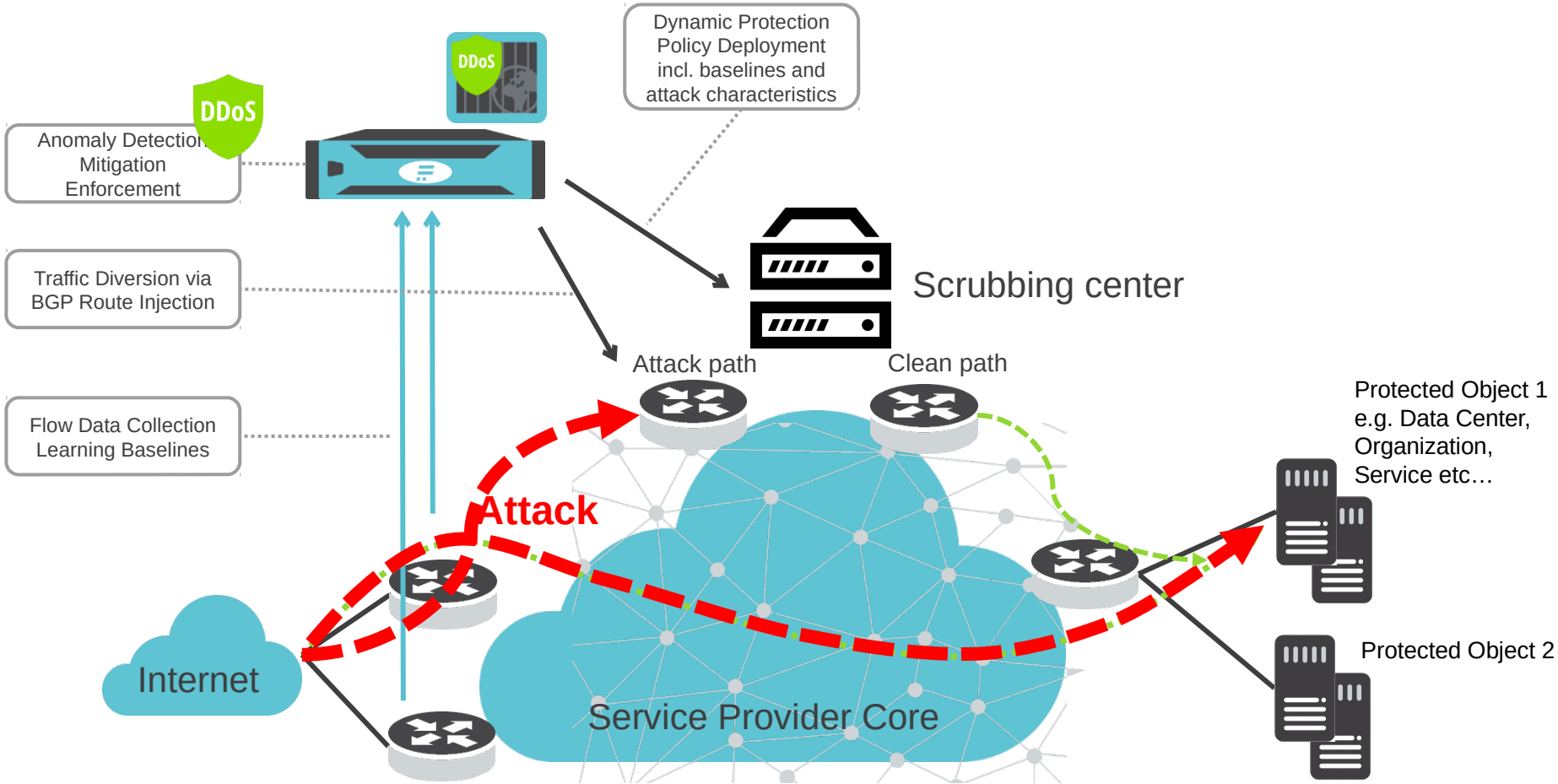
DDoS Protection on Backbone

- Backbone perimeter specifics
  - Multiple peering points – routers & uplinks
  - Large transport capacity – tens of gigabits easily
  - In-line protection is close to impossible!

1. Flow collection
2. DDoS detection
3. Routing control
4. Mitigation control

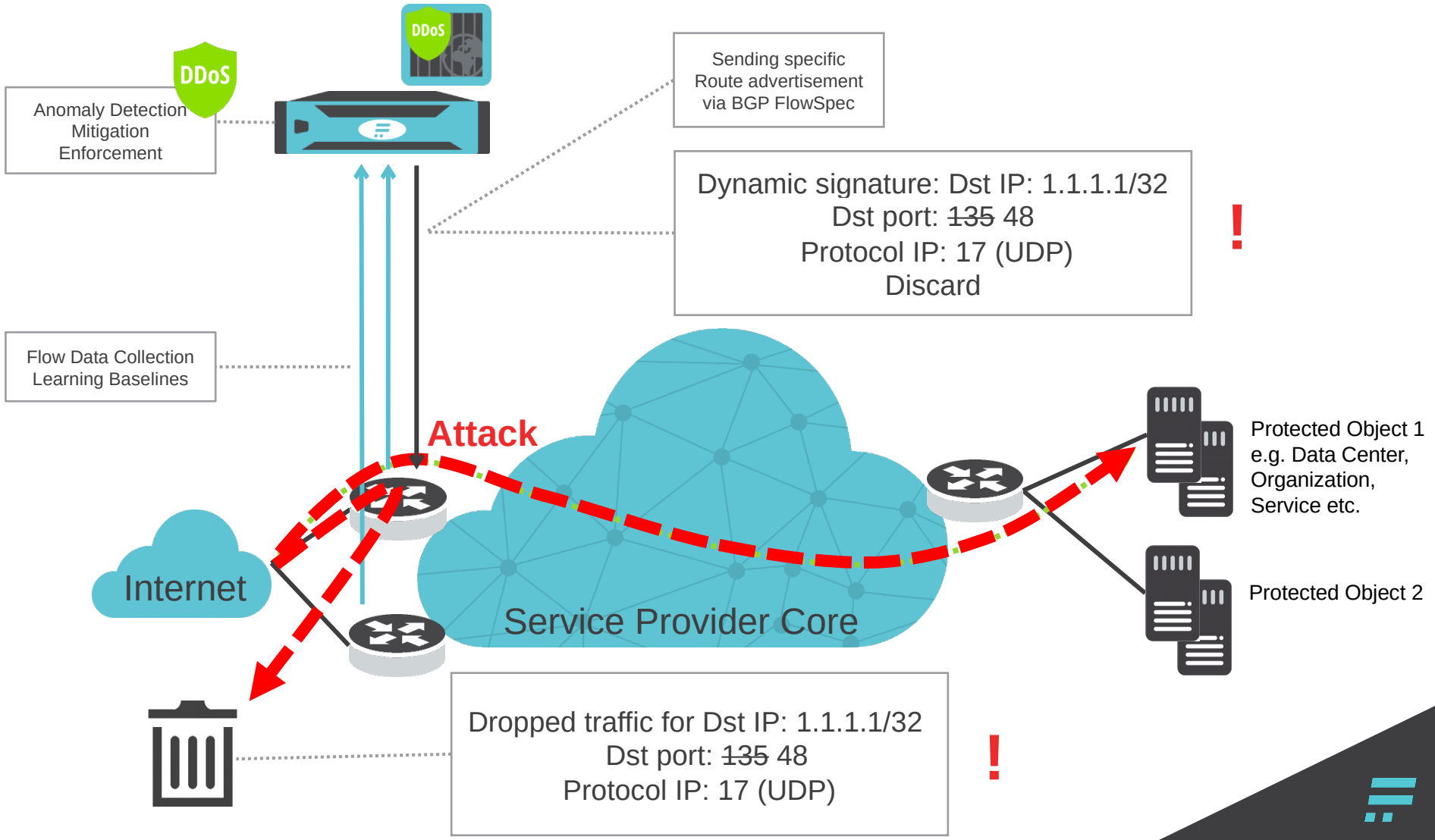
- Flow-based detection and out-of-path mitigation
  - Easy and cost efficient to deploy in backbone/ISP
  - Prevents volumetric DDoS to reach enterprise perimeter

Out-of-Path Mitigation



Flowmon
Driving Network Visibility

BGP Flowspec Mitigation



Flowmon
Driving Network Visibility

Anomaly Detection on Backbone

Anomaly Detection

- Machine Learning
- Adaptive Baselining
- Heuristics
- Behavior Patterns
- Reputation Databases

#	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. 1.52.71.217, 1.52.87.249, 1.52.133.228, 1.52.1 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, 1.52.1 1.52.191.229, 1.52.218.123, 1.52.220.241, 1.52 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, 1.52.44.16 1.52.77.224, 1.52.128.196, 1.52.128.214, 1.52. 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, 1.52.92.1 1.52.174.104, 1.52.183.10, 1.52.184.230, 1.52. 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, 1.52.14 1.52.177.97, 1.53.40.147, 1.53.58.10, 1.53.89. 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: 5.04 MiB, packets: 125 924.	2013-08-24 05:39:59	localhost	1.52.4.138, 1.52.12.103, 1.52.28.61, 1.52.31.7 1.52.42.130, 1.52.44.24, 1.52.48.142, 1.52.67. 1.52.83.34, ...
7	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 3.60 MiB, packets: 88 749.	2013-08-24 03:38:31	localhost	1.52.7.220, 1.52.11.109, 1.52.28.57, 1.52.42.9 1.52.95.134, 1.52.114.14, 1.52.115.205, 1.52.1 1.52.122.10, ...
8	112.90.18.105	L3ANOMALY	The traffic not belonging to any internal network was detected (this may indicate spoofing). Transferred: 2.60 MiB, packets: 63 126.	2013-08-24 03:00:34	localhost	1.52.12.16, 1.52.77.184, 1.52.104.14, 1.52.125 1.52.128.99, 1.52.134.215, 1.52.137.109, 1.52. 1.52.203.143, 1.52.209.197, ...

Flowmon
Driving Network Visibility

FlowMon Reports

Date: 2014-03-21, Location: ads.cdtel.cz, FlowMon ADS ISP 6.05.00

[redacted] - udalosti

Prehled udalosti v siti [redacted]

Time interval: 2014-03-14 07:23 - 2014-03-21 07:23

Priority: **INFORMATION**

#	Source	Event type	Detail	Timestamp	NetFlow source	Targets
1	I [redacted]0.167	BLACKLIST	Known botnet command & control center, attempts: 1, uploaded: 843.00 B, downloaded: 8.28 KiB.	2014-03-21 04:05:16	localhost	54.72.9.51
2	I [redacted]0.167	BLACKLIST	Known botnet command & control center, attempts: 1, uploaded: 883.00 B, downloaded: 8.28 KiB.	2014-03-21 01:55:00	localhost	54.72.9.51
3	I [redacted].161	SCANS	horizontal TCP SYN scan (successful attempts: 6, unsuccessful attempts: 1 192, targets: 1 168, port list: 445, 81, 80, 443).	2014-03-20 23:25:00	localhost	12.1.186.55, 12.10.13.25, 12.12.148.32, 12.35.254.39, 12.61.158.77, 12.81.130.37, 12.113.100.18, 12.117.155.81, 14.23.168.113, 14.32.62.38, ...
4	I [redacted].161	SCANS	horizontal TCP SYN scan (successful attempts: 9, unsuccessful attempts: 1 231, targets: 1 216, port list: 445, 81, 80).	2014-03-20 23:20:00	localhost	12.72.224.61, 14.40.185.42, 14.55.0.69, 14.64.169.96, 14.65.71.9, 14.68.165.90, 14.69.98.28, 14.74.190.26, 14.78.145.76, 14.86.85.90, ...
5	I [redacted].161	SCANS	horizontal TCP SYN scan (successful attempts: 3, unsuccessful attempts: 1 152, targets: 1 133, port list: 445, 81, 80, 139).	2014-03-20 23:15:00	localhost	12.1.60.107, 12.16.188.69, 12.29.238.33, 12.74.220.30, 12.75.189.103, 13.29.16.97, 14.32.158.69, 14.33.65.100, 14.49.106.103, 14.49.122.65, ...
6	I [redacted].161	SCANS	horizontal TCP SYN scan (successful attempts: 3, unsuccessful attempts: 1 096, targets: 1 079, port list: 445, 81, 80).	2014-03-20 23:10:00	localhost	12.43.162.116, 12.63.222.46, 12.69.238.52, 14.54.230.97, 14.61.214.105, 14.62.152.125, 14.71.28.19

Sample Anomaly Detection Report

Focus on Indicators of Compromise

Provided by ISP to Enterprise Customers

Flowmon
Driving Network Visibility

Thank you

Performance monitoring, visibility and security with a single solution

Pavel Minařík, Chief Technology Officer

pavel.minarik@flowmon.com, +420 733 713 703

Flowmon Networks a.s.
Sochorova 3232/34
616 00 Brno, Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility