



DDoS Protection in Backbone Networks

Deployed at Trenka Informatik AG (www.trenka.ch)

Pavel Minarik, Chief Technology Officer

SwiNOG meeting, 9th Nov 2017



Flowmon
Driving Network Visibility

Backbone DDoS protection

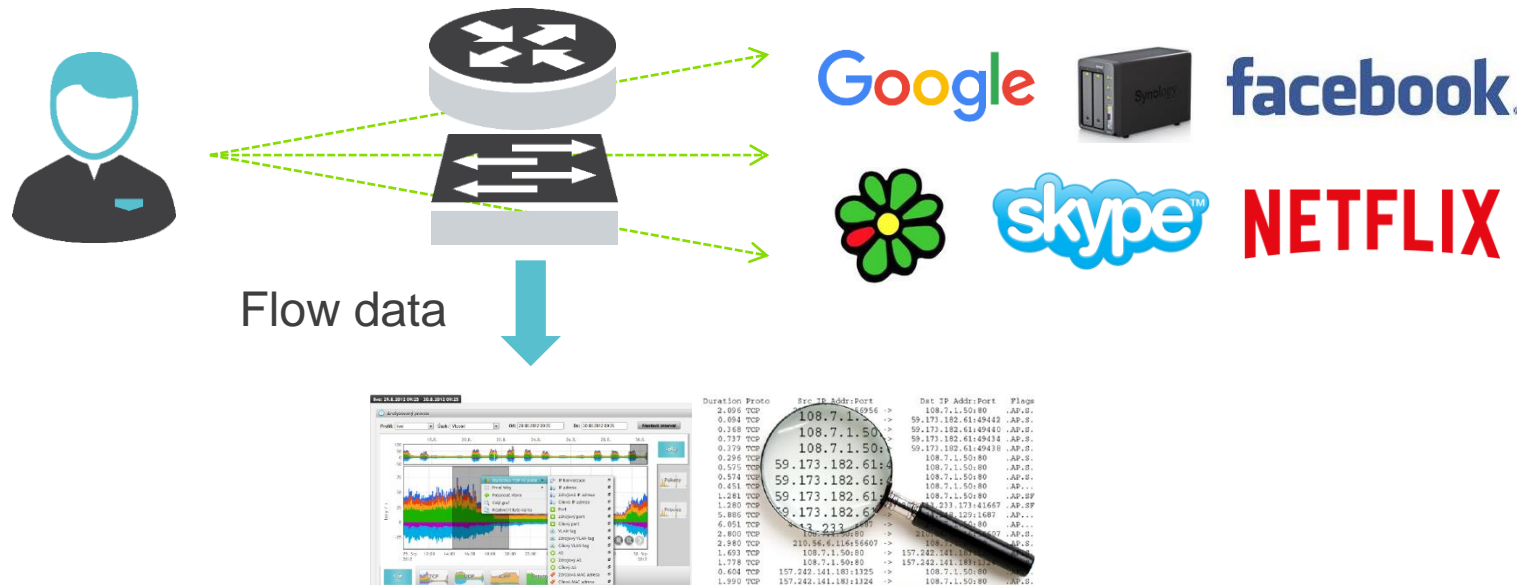
- Backbone protection is specific
 - High number of up-links, network perimeter is wide
 - Massive throughputs – dozens or hundreds of Gbps
 - **In-line solution is out of question!**



- Detection based on **flow analysis** and out-of-path mitigation
 - Simple and cost-efficient solution for backbones
 - Prevents volumetric attacks to reach enterprise networks

What is Flow Data?

- Modern method for network monitoring – flow measurement
- 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



Flow-Enabled Devices

- Network equipment (routers/switches)
 - Traditional capability known for many years



- Firewalls, UTMs, load balancers, hypervisors
 - Ongoing initiative of majority of vendors

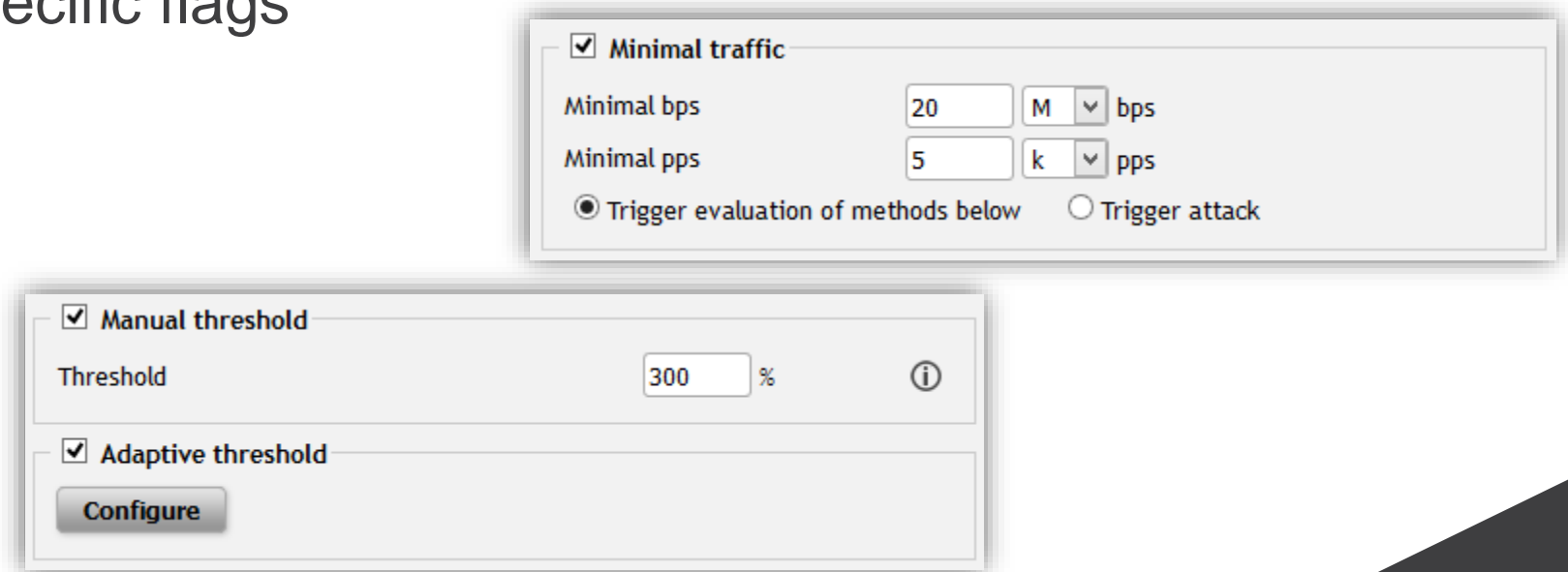


- Packet brokers and matrix switches
 - Convenient option



Attack Detection

- For each segment, a set of **baselines** is learned from real traffic
- Attack is detected if the current traffic exceeds defined threshold
- Baseline is learned for:
 - TCP traffic with specific flags
 - UDP traffic
 - ICMP traffic



The image shows two overlapping configuration windows from the Flowmon interface. The top window is titled 'Minimal traffic' and contains the following settings: a checked checkbox for 'Minimal traffic', 'Minimal bps' set to 20 with a unit dropdown set to 'M' bps, 'Minimal pps' set to 5 with a unit dropdown set to 'k' pps, and two radio buttons: 'Trigger evaluation of methods below' (selected) and 'Trigger attack'. The bottom window is titled 'Manual threshold' and contains: a checked checkbox for 'Manual threshold', a 'Threshold' field set to 300 with a percentage sign and an information icon, a checked checkbox for 'Adaptive threshold', and a 'Configure' button.

☒ Minimal traffic

Minimal bps 20 M bps

Minimal pps 5 k pps

☒ Trigger evaluation of methods below ☐ Trigger attack

☒ Manual threshold

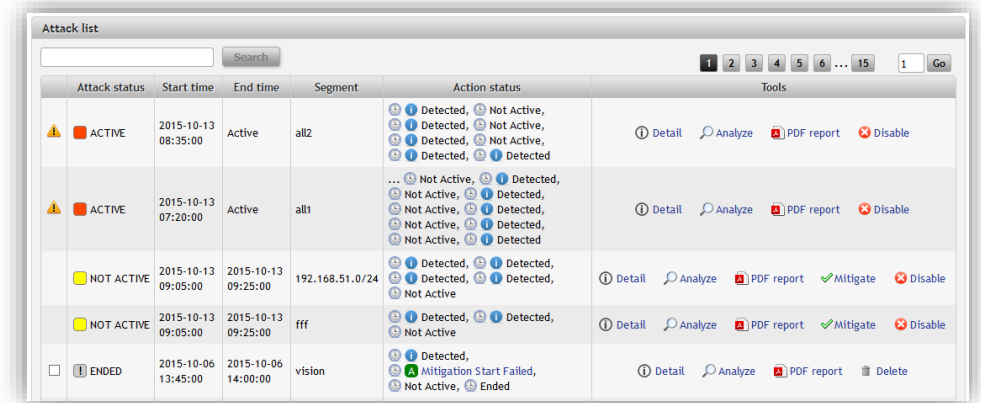
Threshold 300 % ⓘ

☒ Adaptive threshold

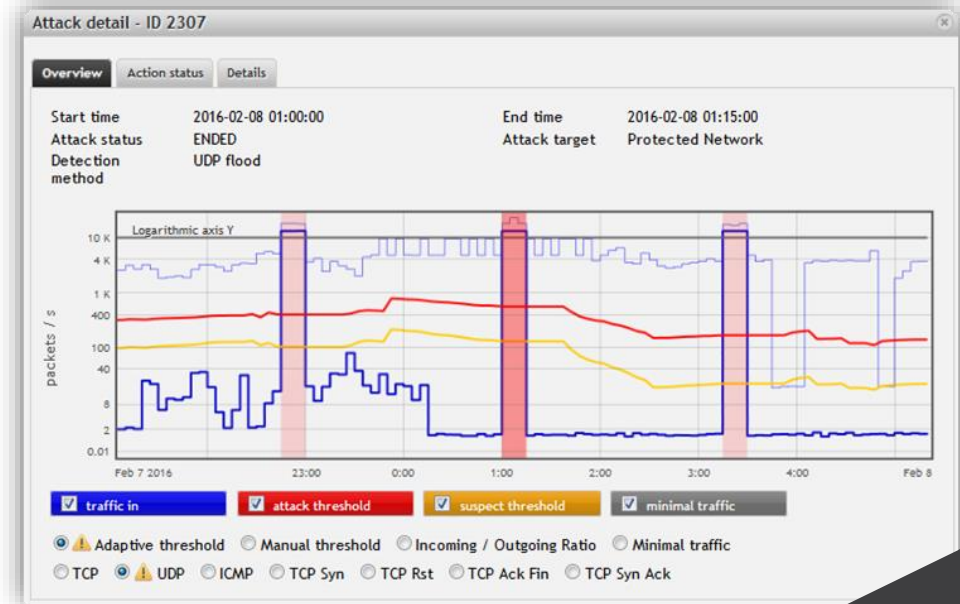
Configure

Attack Reporting

- Start/end time
- Attack target
- Type and status
- Traffic volumes during attack/peace time
- Attack targets (top 10 dst IPs, source subnets, L4 protocols, TCP flags combinations ...)



Attack status	Start time	End time	Segment	Action status	Tools
ACTIVE	2015-10-13 08:35:00	Active	all2	Detected, Not Active, Detected, Not Active, Detected, Not Active, Detected, Not Active	Detail Analyze PDF report Disable
ACTIVE	2015-10-13 07:20:00	Active	all1	Not Active, Detected, Not Active, Detected, Not Active, Detected, Not Active, Detected	Detail Analyze PDF report Disable
NOT ACTIVE	2015-10-13 09:05:00	2015-10-13 09:25:00	192.168.51.0/24	Detected, Detected, Detected, Not Active	Detail Analyze PDF report Mitigate Disable
NOT ACTIVE	2015-10-13 09:05:00	2015-10-13 09:25:00	fff	Detected, Detected, Not Active	Detail Analyze PDF report Mitigate Disable
ENDED	2015-10-06 13:45:00	2015-10-06 14:00:00	vision	Detected, Mitigation Start Failed, Not Active, Ended	Detail Analyze PDF report Delete



Response to Attack

- Alerting
 - E-mail, Syslog, SNMP trap
- Routing diversion
 - PBR (Policy Based Routing)
 - BGP (Border Gateway Protocol)
 - BGP Flowspec
 - RTBH (Remotely-Triggered Black Hole)
- User-defined scripting
- Automatic mitigation
 - With out-of-band mitigation devices
 - With services of Scrubbing centers

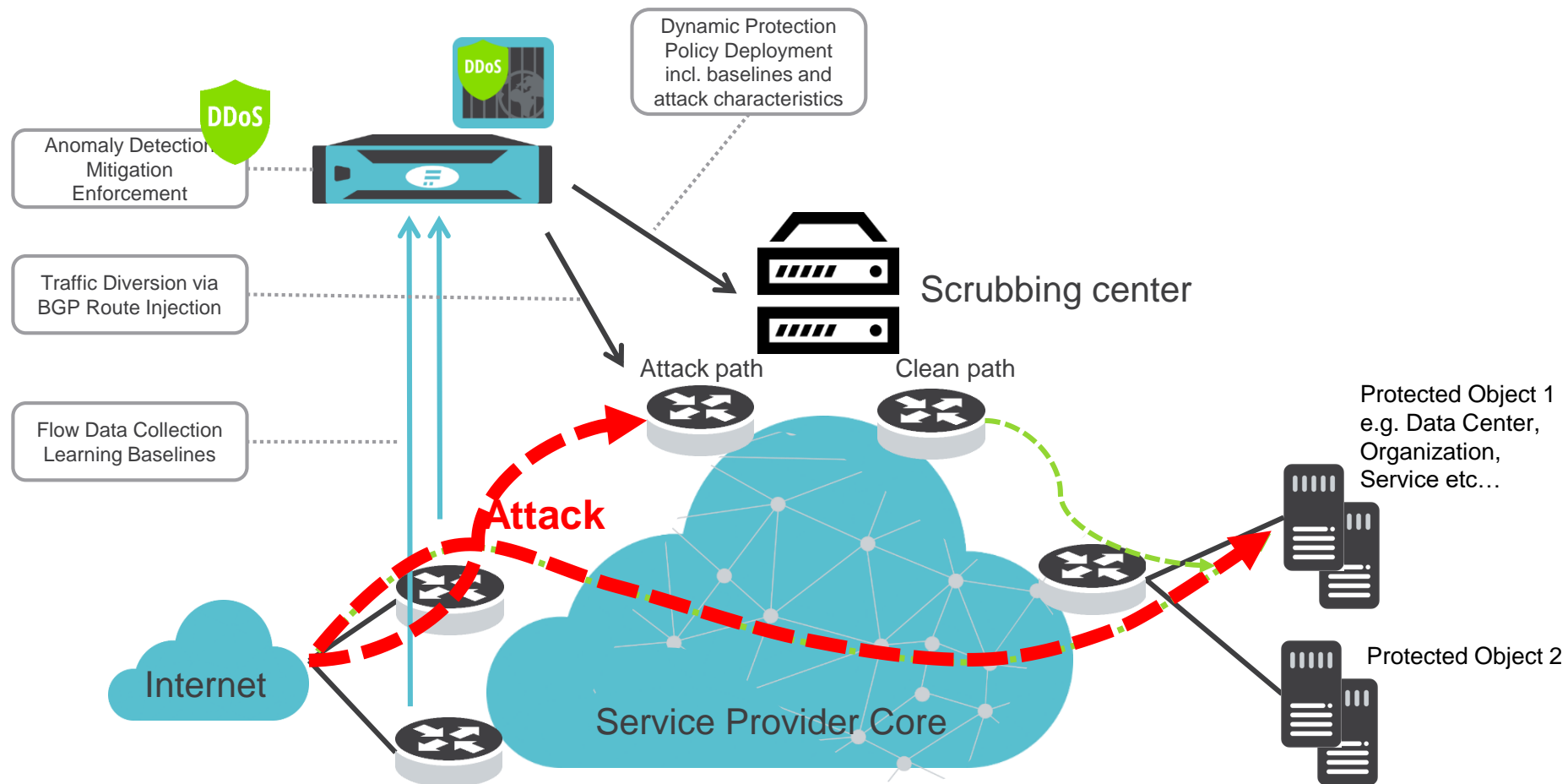




DDoS Protection Scenario 1

Out-of-path Mitigation

Out-of-Path Mitigation



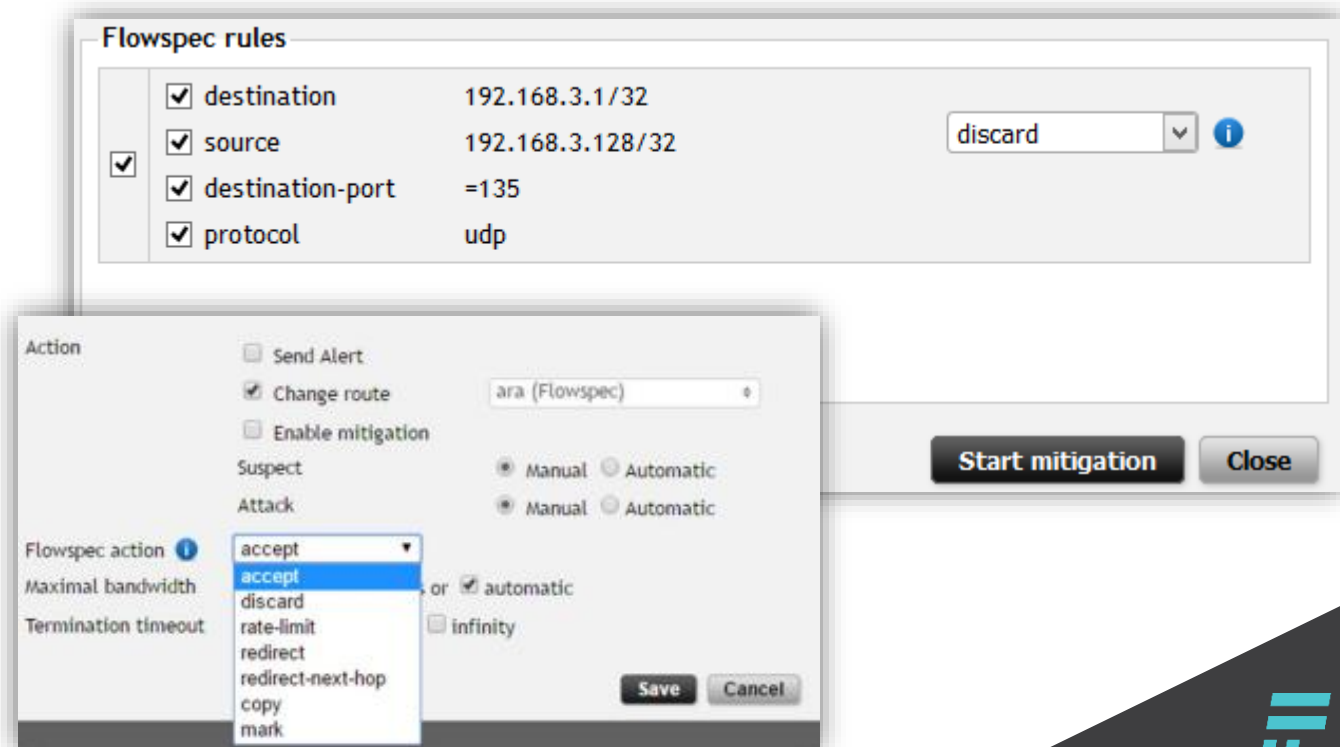


DDoS Protection Scenario 2

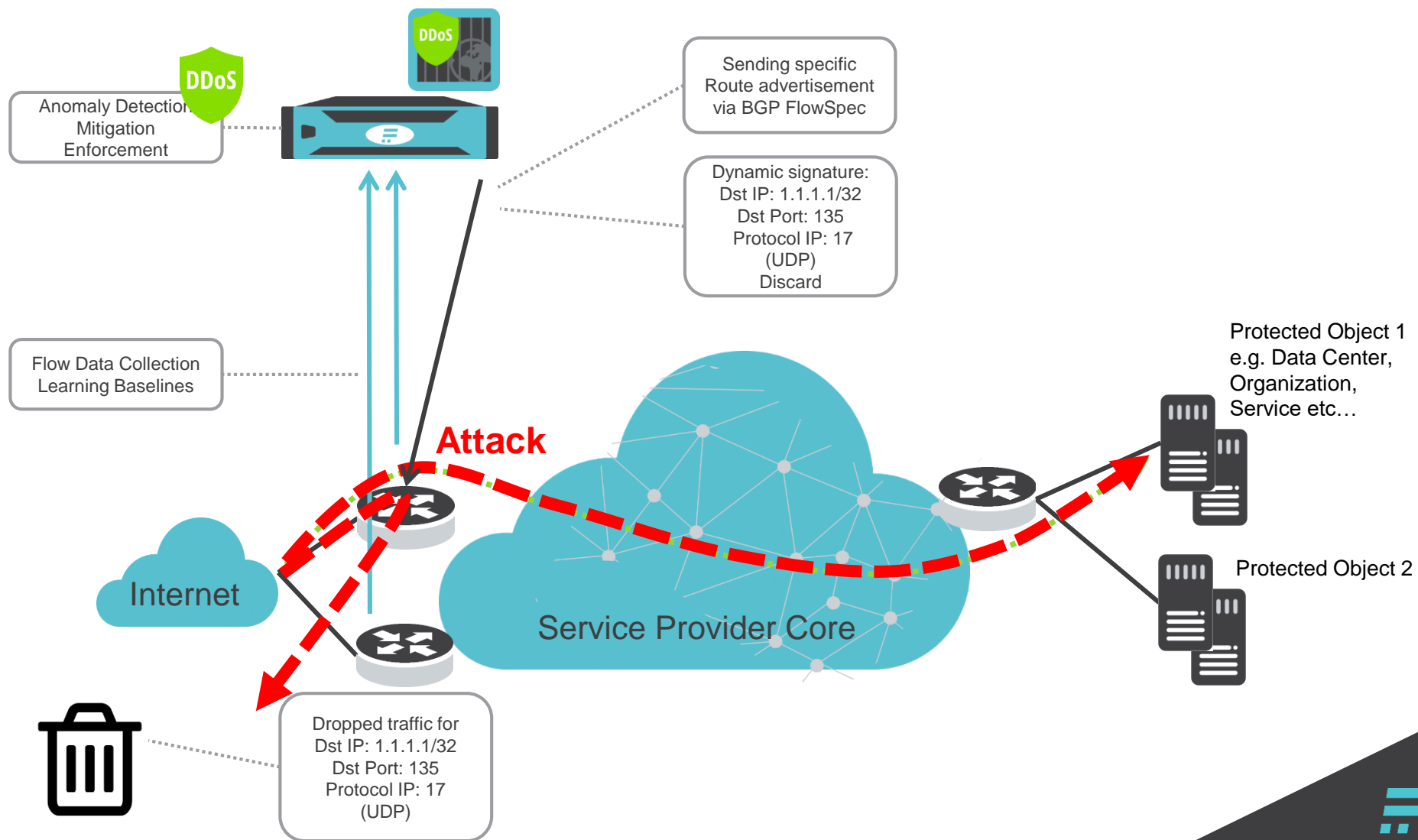
Mitigation with BGP Flowspec or RTBH

BGP Flowspec or RTBH

- Based on **dynamic signature** of the attack
- Provides **specific action** to take with network traffic
- BGP Flowspec rules are based on
 - Destination Prefix
 - Source Prefix
 - IP Protocol
 - Destination port
 - ICMP type
 - ICMP code
- RTBH is pure BGP



BGP Flowspec or RTBH Scenario





Demonstration

DDoS Protection Deployed at Trenka Informatik AG

Trenka Informatik AG



- Office in Zürich, more than 20 Years network experience
- Backbone in 3 data centers in Switzerland, AS29655
- Provide solutions for IT- and ISPs
- Competent network team
- Flowmon integrator
- Contact

tel: 044 383 6307
e-mail: admin@trenka.ch



Milan Trenka
Dipl. Ing. HTL

Summary

- Flow data enable quick detection and response to DDoS attack (primarily volumetric)
- Appropriate aggregation rates and sufficient detail
- Detection and mitigation can be automated
- We can't get rid of all attacks, but their impacts can be reduced





Thank you

Performance monitoring, visibility and security
with a single solution

Pavel Minarik, 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