IP-Plus DDoS Protection Service

IP-Plus Engineering

swisscom

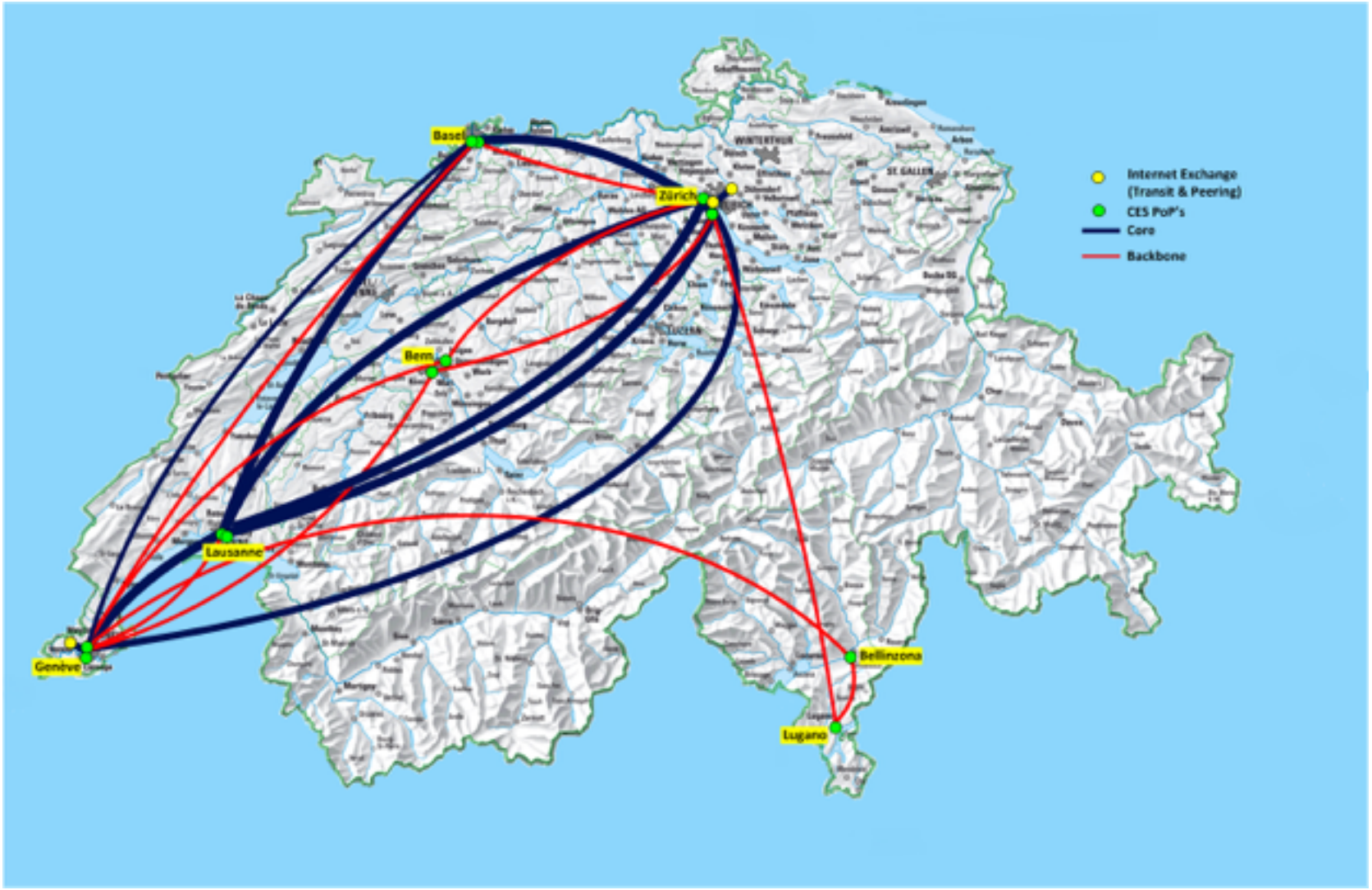
IP-Plus Overview

some Fun Facts

- Largest Swiss ISP, founded as Uniplus in 1995 when Switch had to sell its commercial customers to PTT/Unisource Business Networks.
- mainly Corporate customers, connected through VDSL and CES (Carrier Ethernet Service)
- Residential and SME customers served through ex-Bluewin
- Upstream for all Swisscom services
- For 20 years we remained MPLS-free (but recently we enabled LDP for Asian routes)
- IPv4/IPv6 dual-stack for many years.
- All interfaces are in a public but not globally routed IP range.
- COPP to limit access to the routers control plane.

Swisscom IP-Plus® Internet Backbone

Switzerland



swisscom

Swisscom IP-Plus® Internet Backbone

Asia

Swisscom IP-Plus® Internet Backbone

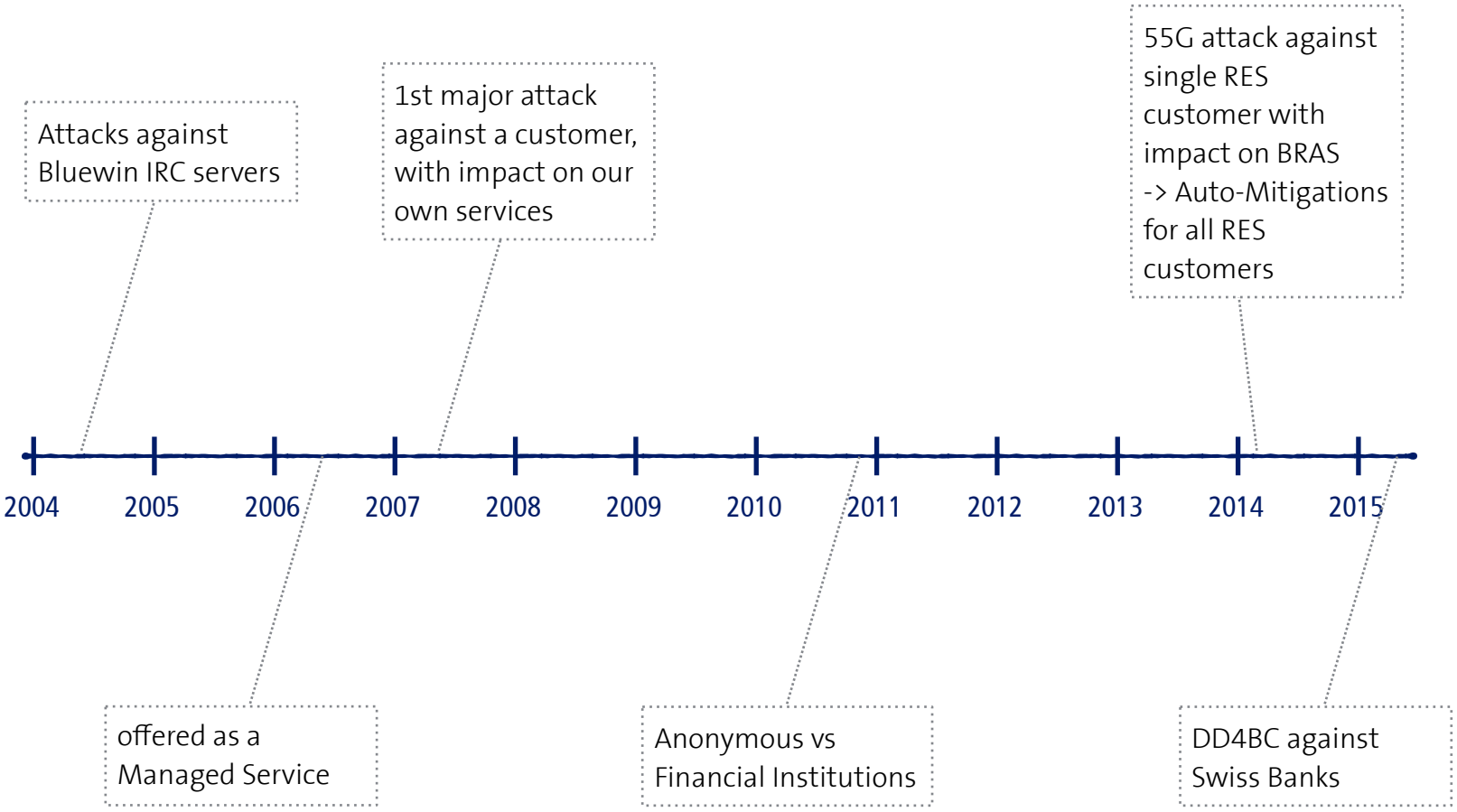
North-Atlantic

swisscom

DDoS Protection Overview

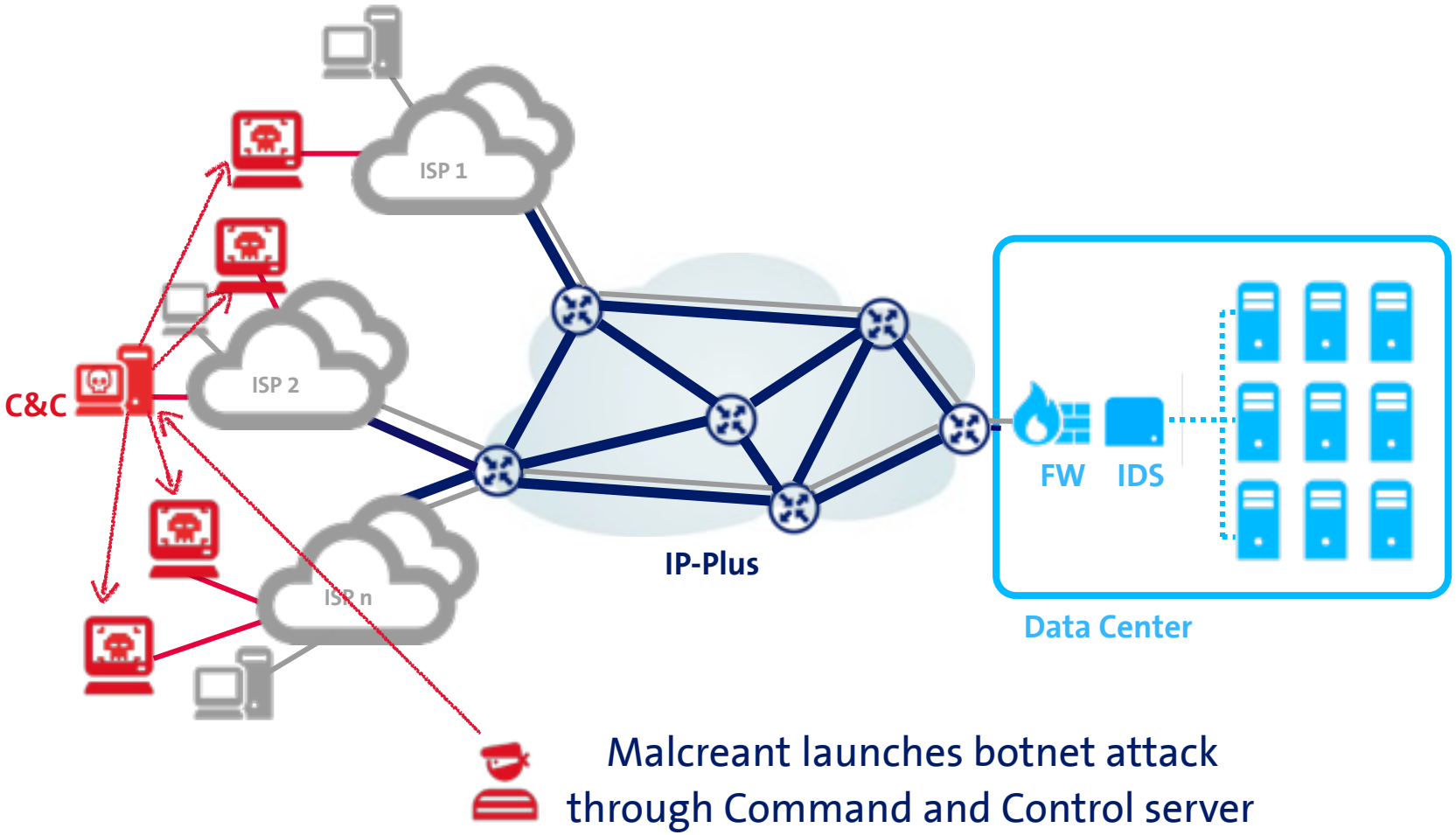
IP-Plus® DDoS Protection Service

since 2004



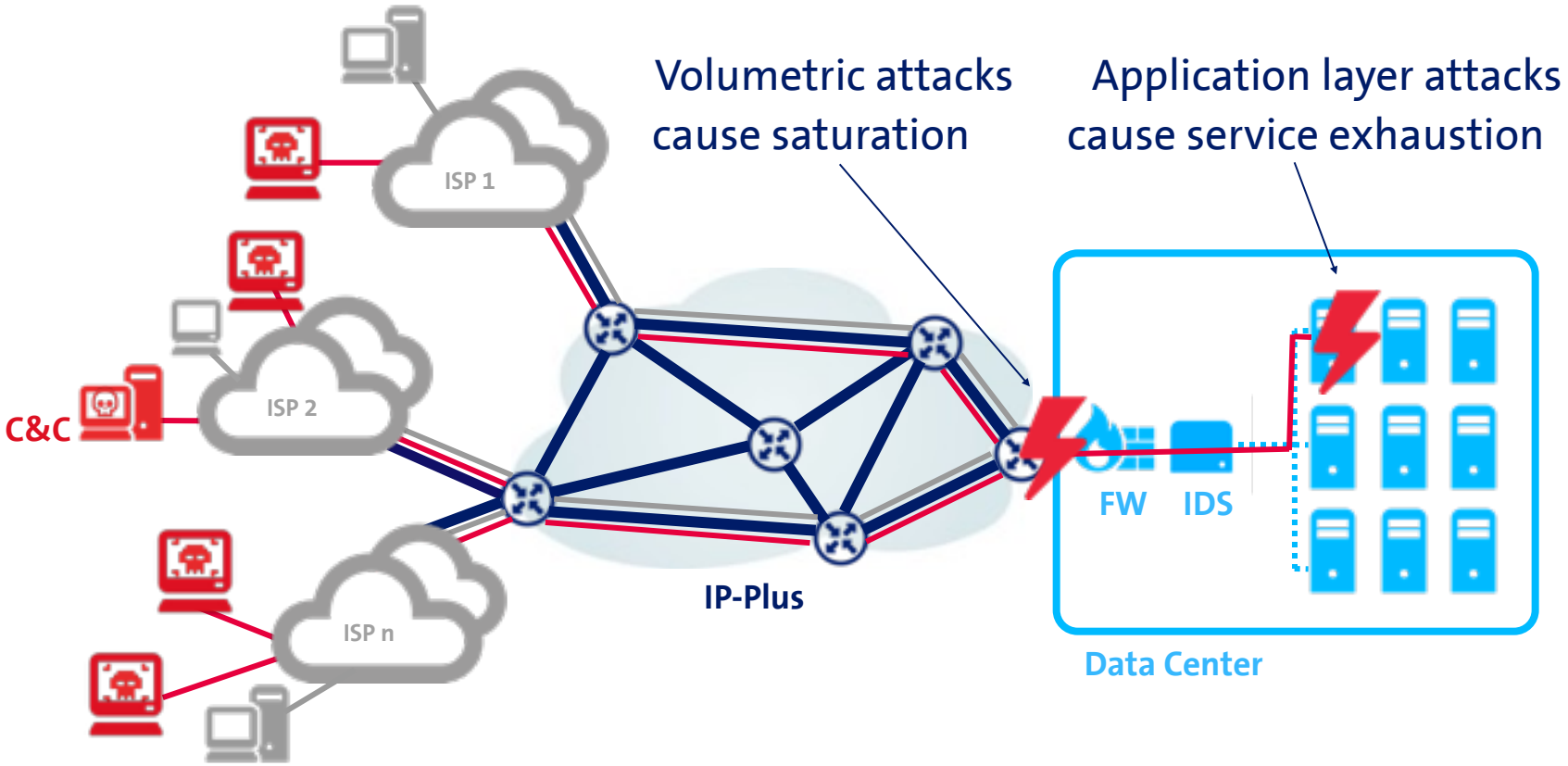
swisscom

Schematic of a Botnet Attack



Malcreant launches botnet attack
through Command and Control server

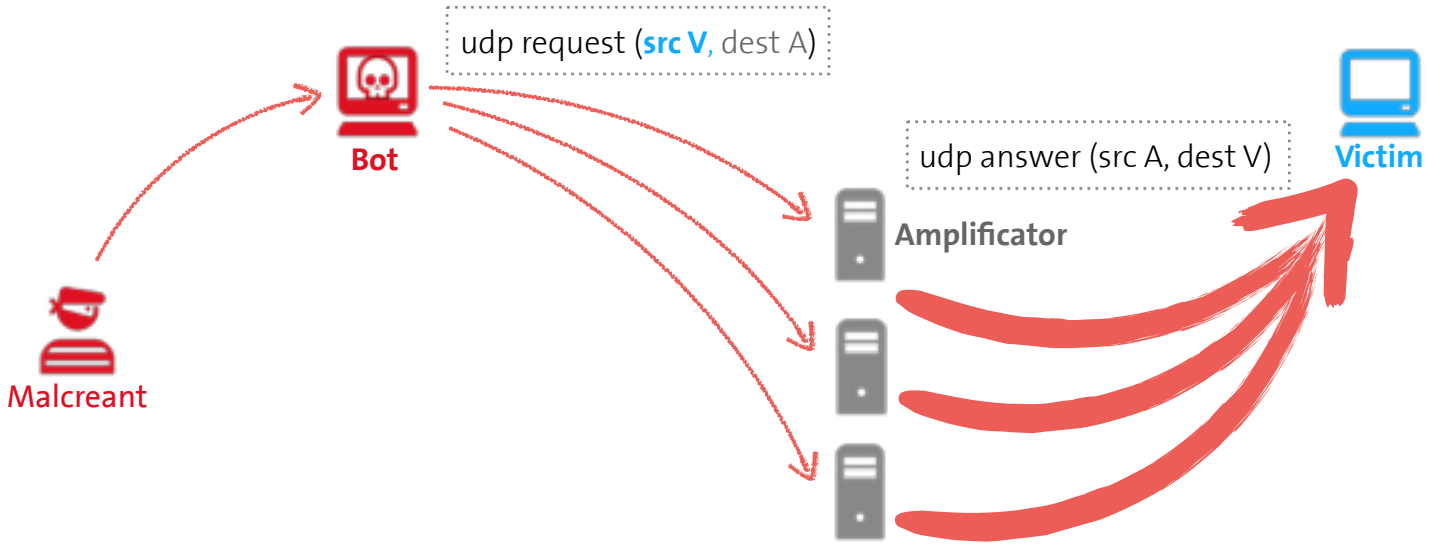
Schematic of a Botnet Attack



No (easy) traceback to C&C or malcreant

The latest flavor: Amplification Attacks

Abuse of unprotected udp services



- source IP spoofing is still one of the biggest problems in the Internet
- only remedy is BCP38

Amplification Attacks

- reflective DNS attacks: queries for ANY on open resolver
- NTP amplification attacks: queries for monlist on older ntpd
- unprotected SNMP daemons with default community string
- other unprotected (mostly legacy) udp services: qotd (udp/17), chargen (udp/19), ssdp (udp/1900)
- and since august RPC port mapper (udp/111)
- as a first line of defense we rate-limit these udp services at our Peering edge

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]
NTP	556.9	see: TA14-013A [2]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

Attack Size

- Our largest attack so far was around 55 Gbps, current attacks in the Internet are over 400 Gbps:

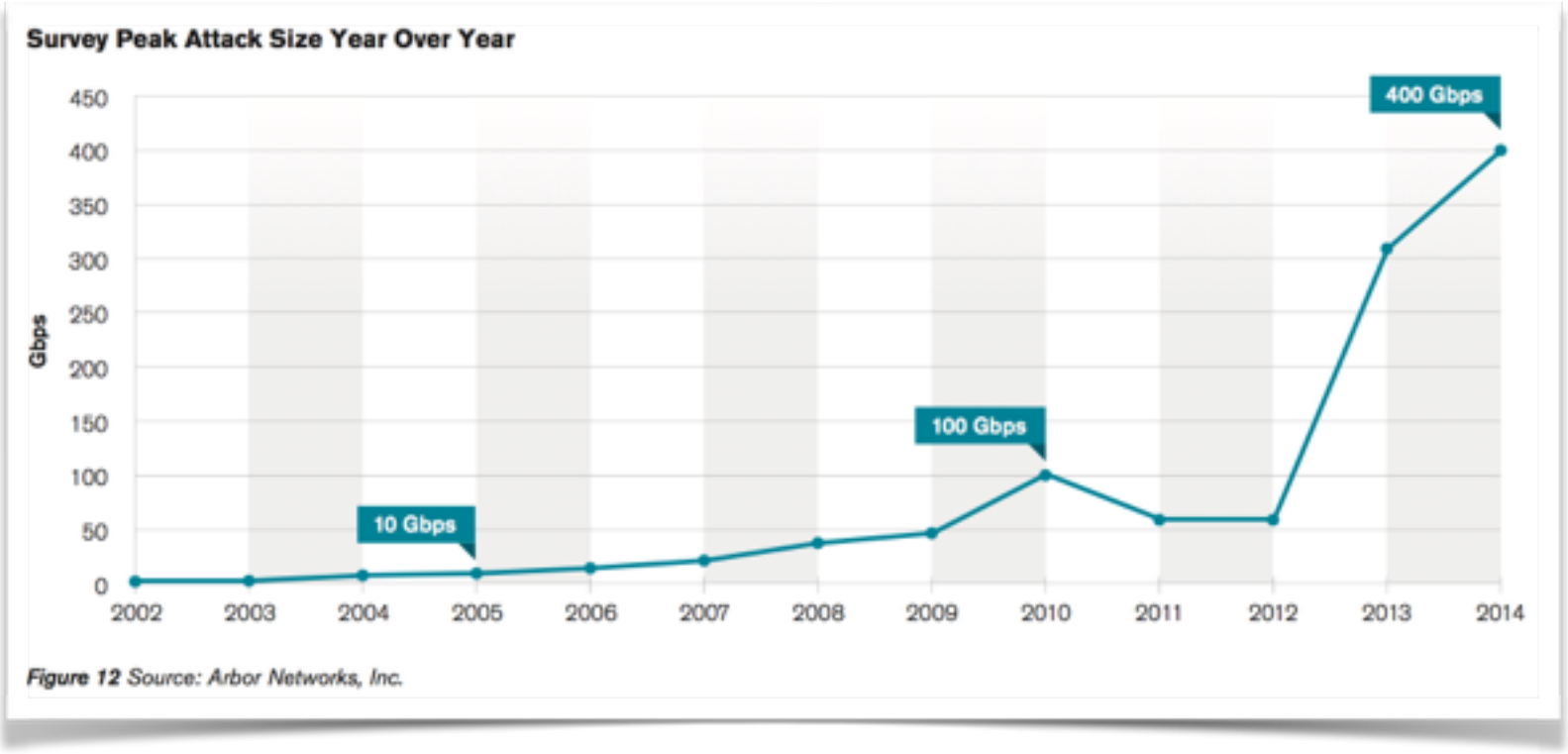


Figure 12 Source: Arbor Networks, Inc.

Application Layer Attacks

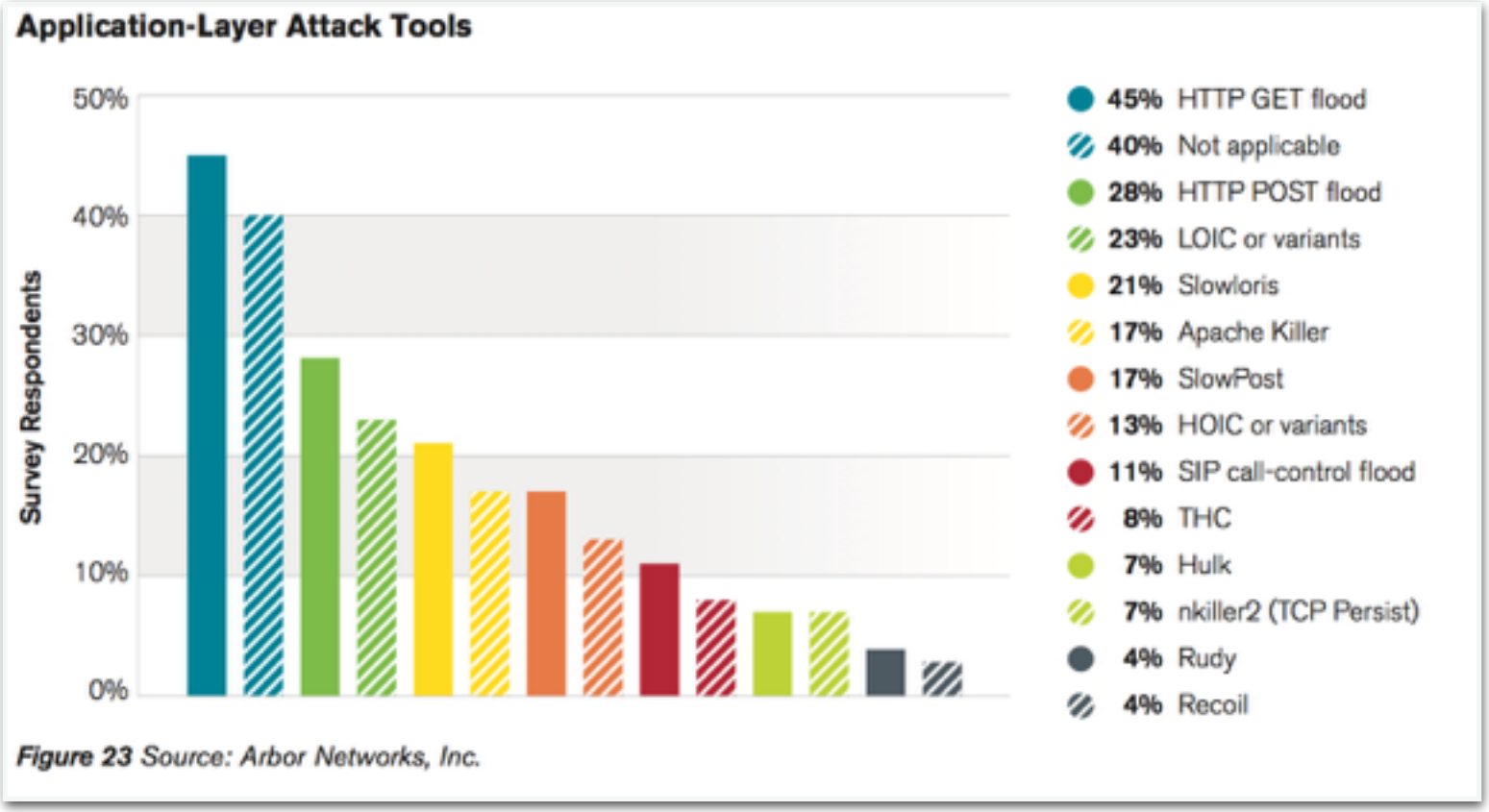


Figure 23 Source: Arbor Networks, Inc.

Attack Motivation

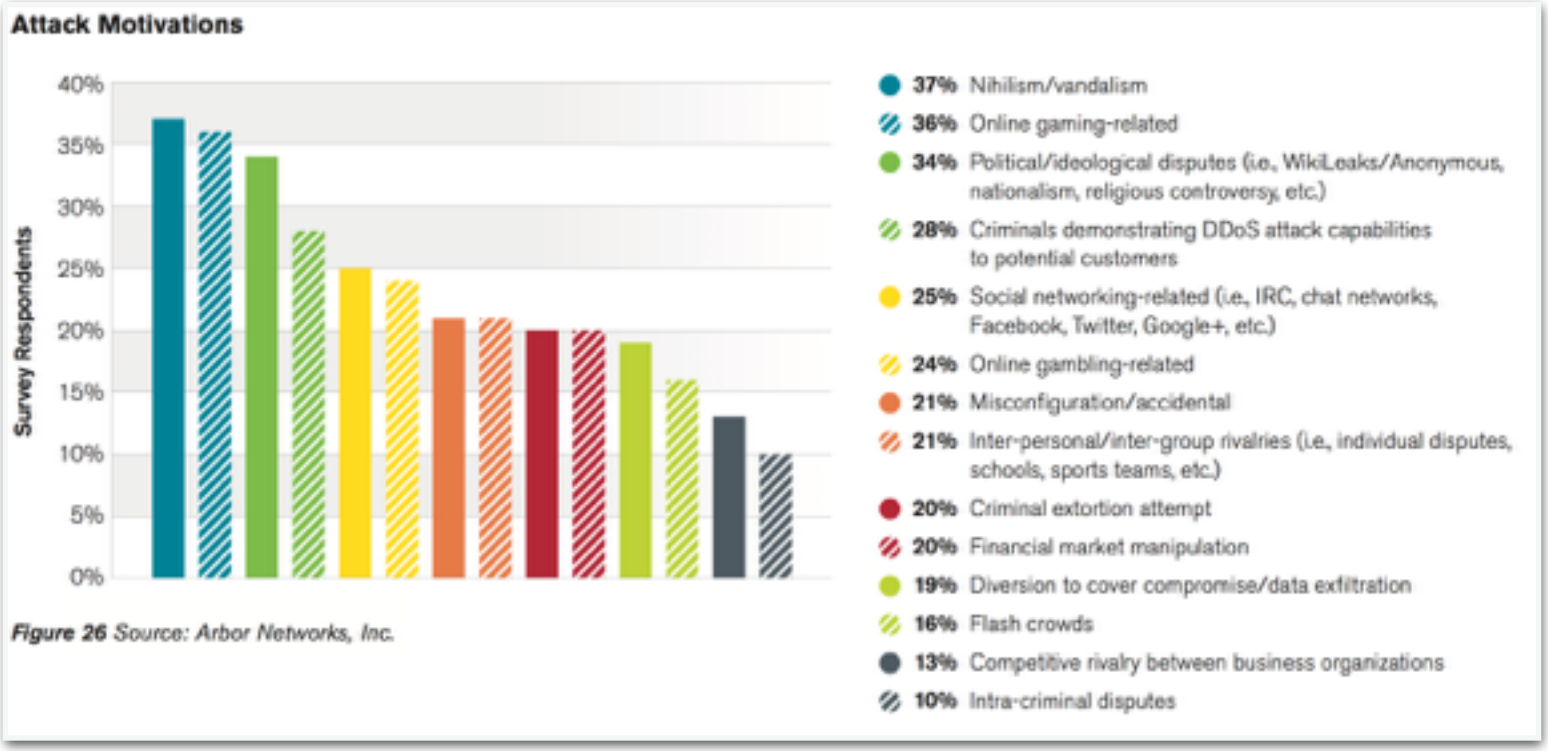


Figure 26 Source: Arbor Networks, Inc.

swisscom

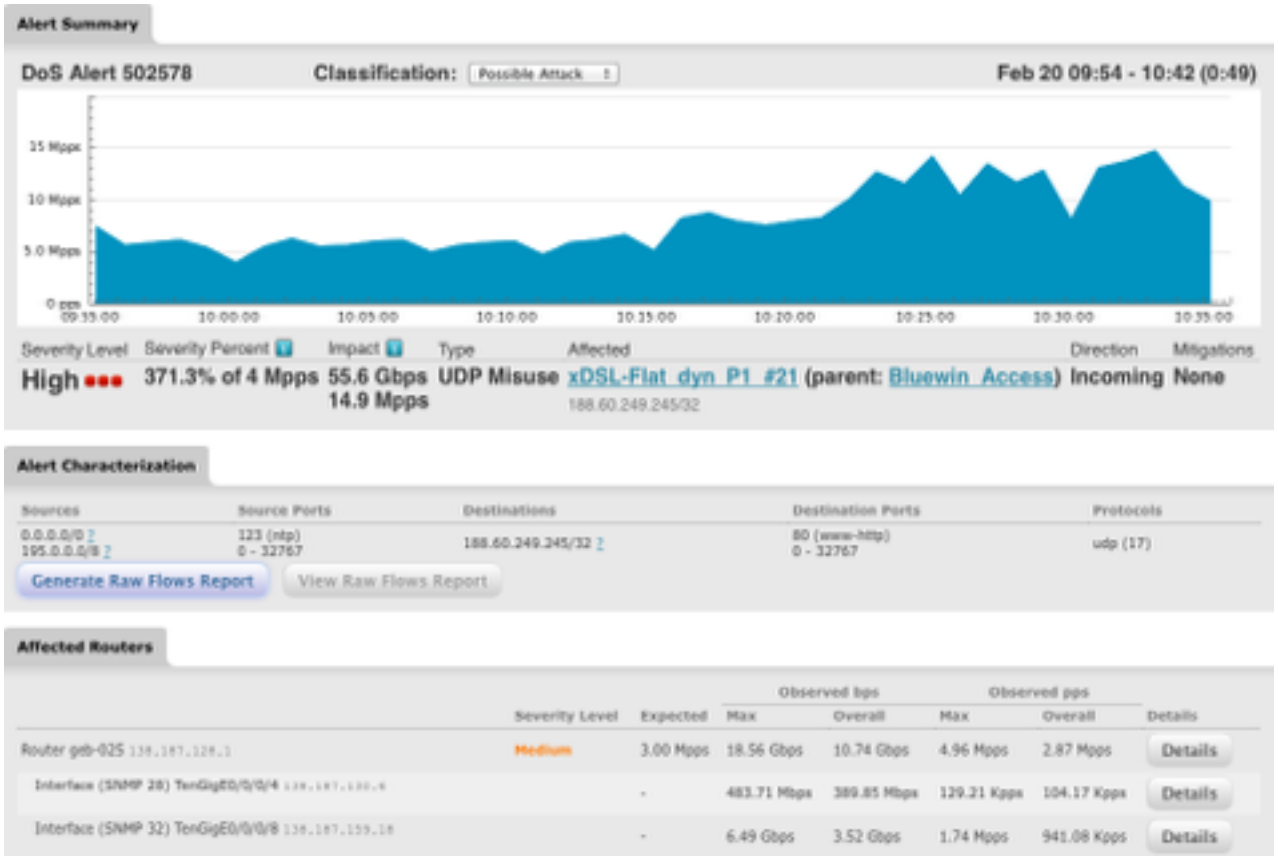
Threat Detection

- Our DDoS Protection platform detects and classifies DDoS attacks and other threats/anomalies against customers and infrastructure
- We collect Netflow (sampled 1/1000)/BGP/SNMP data at all Peering edge and core routers and correlate these —> Detection only up to Layer4

- **Detection methods:**
  - Misuse Detection
    - based on threshold for a set of packet types
  - Profiled Detection
    - based on deviation from baseline (usual traffic behavior)
  - LocationIP Detection
    - Alert on traffic spikes from unexpected countries

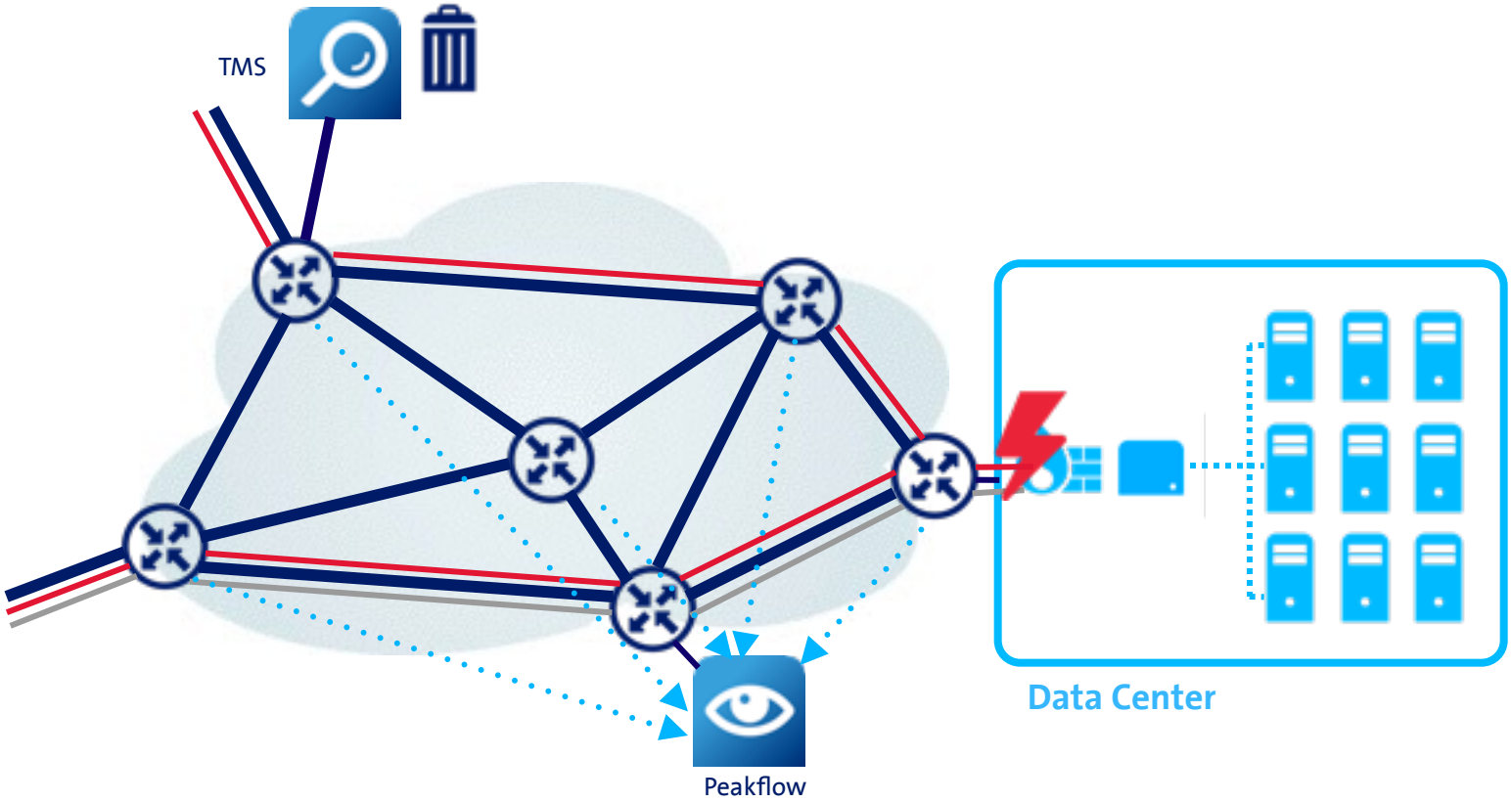
2nd Level Anomaly Reports

- Characterization shows the major components involved in each anomaly
- Graph shows how traffic compares to expected rates
- Links to raw flow queries, mitigation and reporting options for the anomaly



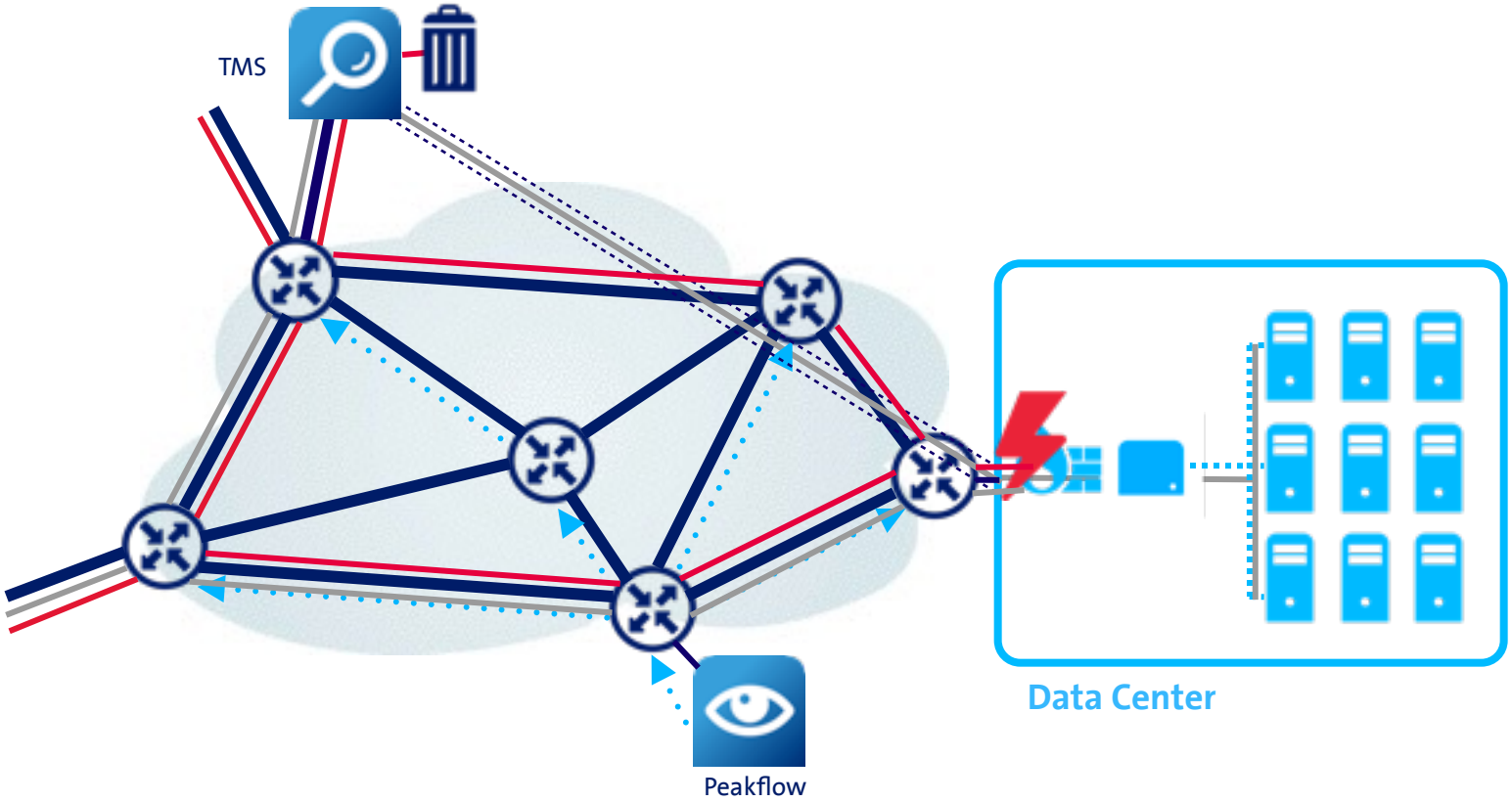
swisscom

Threat Mitigation



Peakflow receives Netflow, BGP and SNMP information from all edge and core routers, correlates this information and raises an alert (email, SMS, Syslog...) if a **high** anomaly is detected. No auto-mitigation will be started!

Threat Mitigation



If an operator decides to start a mitigation, Peakflow injects a BGP host route for the attacked IP with the TMSs address as a new next-hop
—> traffic flows now to the TMS instead, is mitigated and re-routed through a tunnel directly to the customer‘s CPE.

Threat Mitigation - The Countermeasures

- Once the traffic flows through the TMS we have full DPI capabilities to analyze the traffic
- TMS offers a rich set of permanently growing and highly sophisticated countermeasures for surgical and effective mitigation
- e.g.
  - Black / White Filter Lists
  - Zombie Removal
  - TCP SYN Authentication (Multiple)
  - LocationIP Policing
  - SSL Negotiation Filtering
  - ...