Xantaro
SERVICE INTEGRATION

DDOS ATTACKS IN THE REAL WORLD

HOW TO MITIGATE THEM

Who Am I?

- Tobias Heister
- Solutions Architect
  - Technical Pre-Sales
  - Vendor MGMT for Focus Vendors
  - Solutions Engineering and Partner Evaluation
  - XT3LAB

- 3y Deutsche Telekom – Carrier and DC
- 8y Host Europe - Hosting Provider, Network centric Roles (Engineering, Managed Services)
- 3y Xantaro – Professional Services for 1y then SOLAR

Who are We?

- **Our core competency is SERVICE INTEGRATION** –
  the development and integration of solutions across technological and corporate boundaries.
- We plan, implement and maintain the networks and services of our customers, thereby supporting their business success.
- For our customers, we are their **TRUSTED ADVISOR** and the „**NO-WORRY-COMPANY**“, that inspires and creates an ultimate level of trust through absolute customer and service focus, ambitious execution, technical expertise and quality.
- 150 People (135 DE, 15 UK), >70% technical

OUR TECHNOLOGY SOLUTIONS –
Covering All Network Layers

Xantaro SERVICE INTEGRATION

ORCHESTRATION & AUTOMATION	CLOUD AUTOMATION	AUTOMATIC DEVICE & SERVICE PROVISIONING	SERVICE LIFE CYCLE MANAGEMENT	SERVICE DESIGN

VALUE-ADDED & CENTRAL SERVICES	EPC	IMS	xPLAY	VPNs	DHCP	DNS	AAA	BILLING	ANALYTICS	CLOUD SERVICES

SESSION CONTROL & PROTECTION	FIREWALL	SESSION BORDER CONTROLLER	BROADBAND NETWORK GATEWAYS	LOAD BALANCING	DDOS MITIGATION

INFRASTRUCTURE ABSTRACTION	SOFTWARE DEFINED NETWORKING (SDN)	NETWORK FUNCTION VIRTUALISATION (NFV) DATA CENTRE INFRASTRUCTURE ABSTRACTION

INFRASTRUCTURE	ROUTING	SWITCHING	ACCESS (RADIO / WIFI)	OPTICAL TRANSPORT & ACCESS	STORAGE	COMPUTE	DATA CENTRE NETWORKS

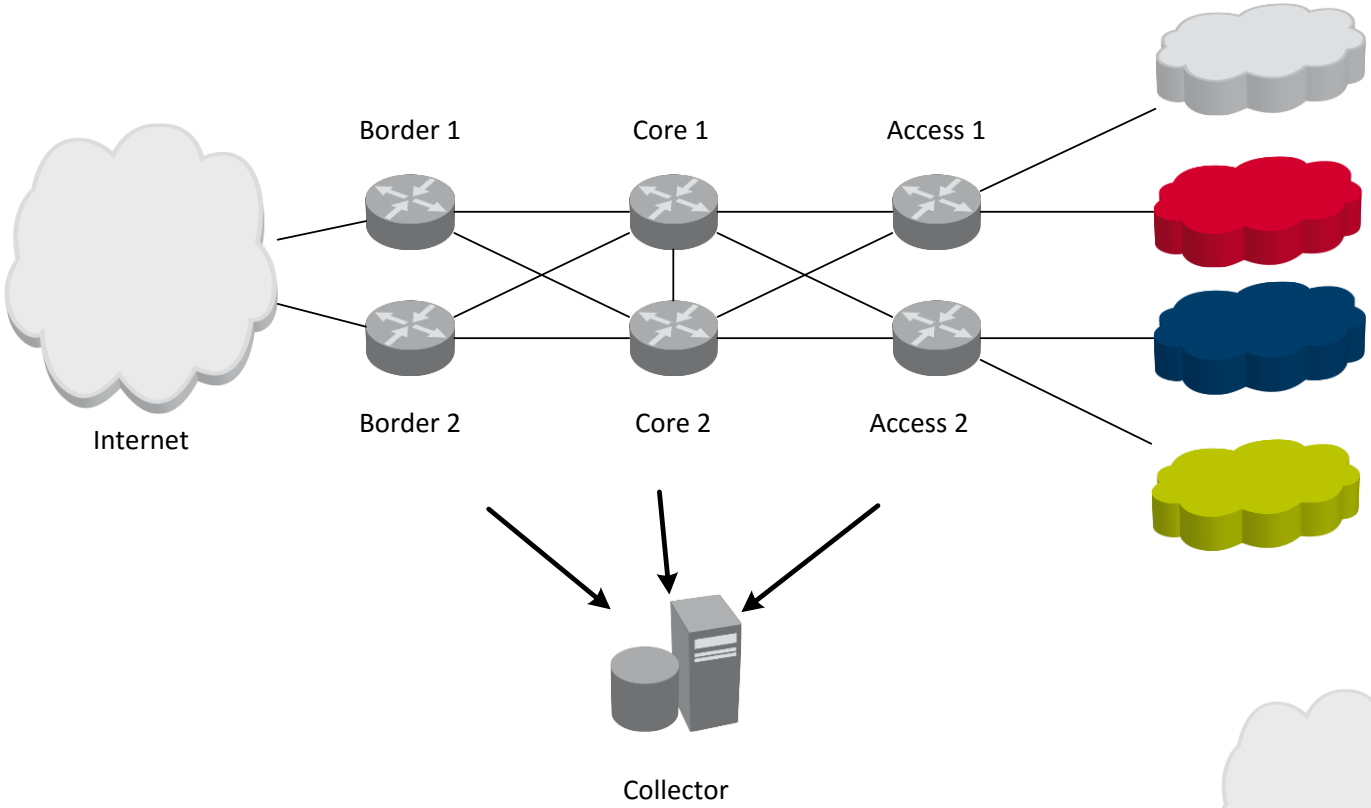
Attacks now and then

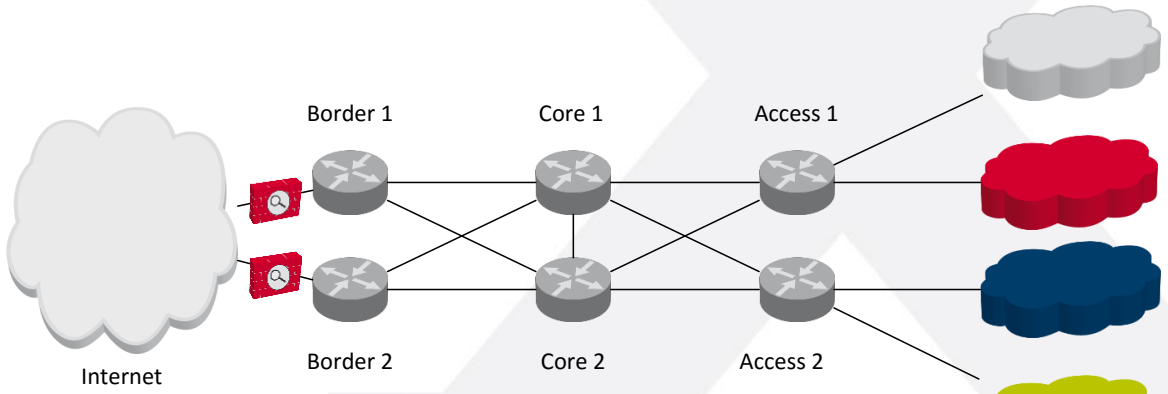
- DoS to DDoS
  - Ping of Death
- Volumetric Attacks
  - UDP based (no state on attacker side)
  - Reflection (Initiator does not attack directly)
  - Spoofed Sources
- Application Layer Attacks (Low and Slow)
  - Consume/Saturate Resources or Time Slots (Tar pitting, Slowloris)
  - State Exhaustion (Connection Tables, Memory, available Processes)
  - Scanning/Reconnaissance (find Vulnerability, weak passwords)
- Combinations
  - Volumetric Attack used as Smoke Screen
  - Targeted Application Layer Attack or Exploit/Hack

You can only fight what you see

- First Step is Detection (which has to be as automatic as possible)
- Multiple ways
  - Log Files, Flow Exporting, Customers Calling, Inline Solutions
- Volumetric Attacks have visible impact and Collateral Damage for the network
  - 250G coming into a 10G pipe will create Service Loss for everyone
  - Can take out entire network/infrastructure
- Application Attacks take out a specific service but may not be visible
  - Slowloris attack on single Webserver will not be noticeable on NOC Dashboard
  - Will likely hit single customers/service

Typical Detection Scenarios



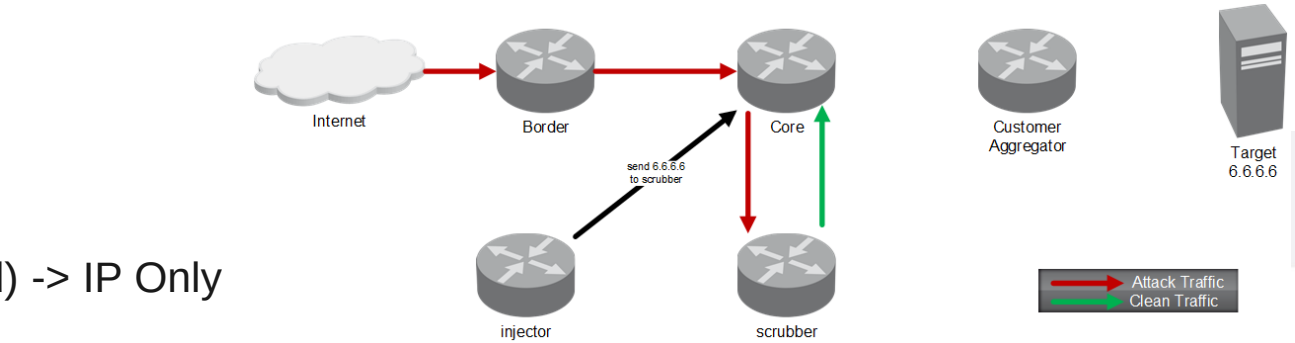


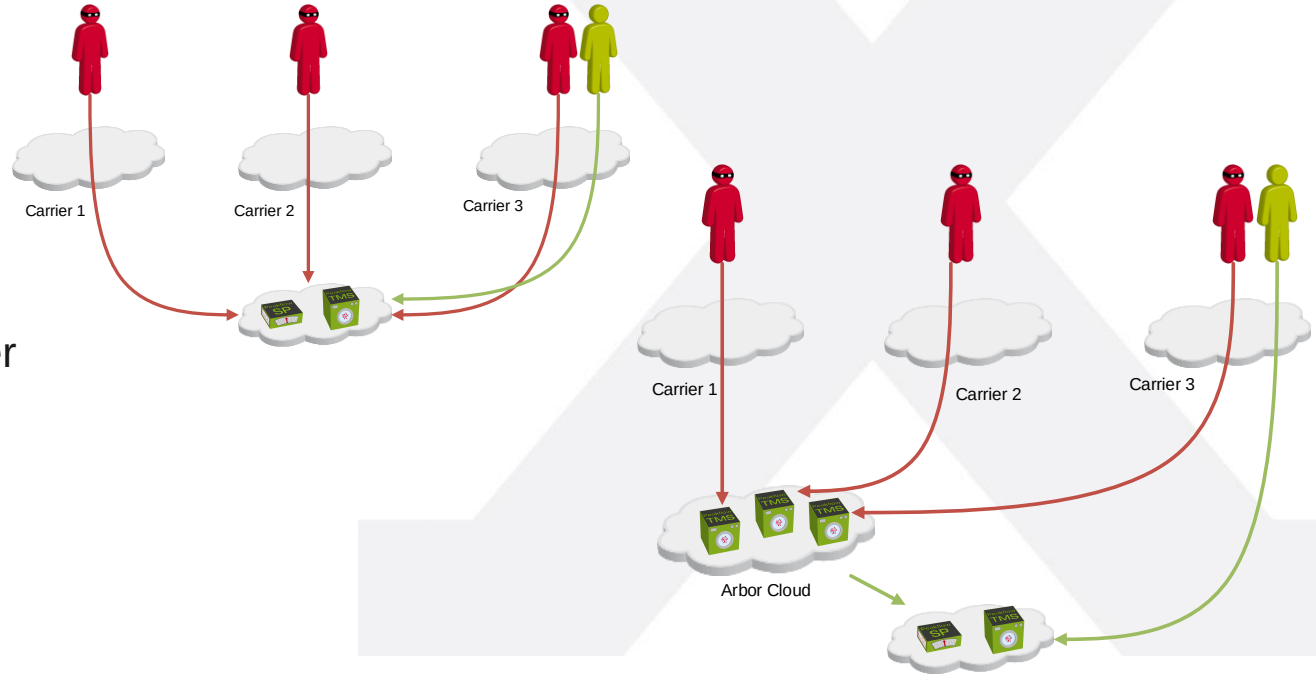
How to detect

- Most Systems available work on Thresholds
  - Defined per Segment/Customer/Network/Prefix per Protocol/Features/Behaviour Limit for $timeframe
  - What is normal? Do the limits change over time?
- Some Systems provide Profiling
  - Learn for a period of time defined as normal, if specific threshold over normal -> alarm
  - (automatically) re run Profiling
  - How to make Sure that Profiling does not take place during attack? What if threshold level is triggered by valid event? (AD Campaign, $event, …)
- Fingerprints (Somebody knows it is bad so i can drop it without checking)
- Artificial Intelligence
- Escalation on Volume/Impact, if Threshold is X for Ymin and Impact is 100 times X reduce monitored timeframe
- We can only analyze what we see (Flow Exporting and Sampling vs. Inline)

Remove Threats

- Once Threats are detected we can do something
- Network centric
  - ACL/Firewall Filter
  - Remote Triggered Blackholing (if possible source based) -> IP Only
  - BGP Flow Spec -> IP/Proto/Port and a bit more
- Attack centric
  - Redirect/Off-Ramp Attack to Scrubbing Appliance
  - On-Ramp Cleaned Traffic
- External Help
  - Remote Triggered Blackholing send to Upstream/Carrier
  - BGP Flow Spec send to Upstream/Carrier
  - „Cloud based“ Mitigation (works only for >= /24 or /48)





Countermeasures

- Once detected and send to Mitigation Appliance we can analyze further (>= Layer4)
- Common Countermeasures
  - Basic Compliance, valid IP, TCP, UDP, ICMP, Checksums
  - Syn Authentication (OOS Ack, Redirect, Cookies)
  - Rate Limiting for BW, Connections (What is good? What is bad)
  - Regional Blocking (For a German Web shop DACH may be fine, the Rest of the World can stay away)
  - Protocol Compliance
    - Valid Verbs/Actions or Syntax
    - Reasonable Amount of Objects/queries
    - Strict/Loose RFC Handling
    - Timeouts
  - Proxy/CGNAT Handling (Client Identification)
  - SSL Handling, Handshake Compliance, Decrypt SSL?

Countermeasures

- Common Countermeasures (continued)
  - Payload Analysis
    - Which DNS queries are valid (do we need to allow ANY queries?)
    - Regular Expression against Payloads (e.g. Fingerprints, Custom Expressions)
    - Bit/CodePoint of Death
  - Create enough Statefullness to identify threats
    - Reflection Attacks (lots of answers without any questions)
    - Slowloris
  - But keep Statefullness to a minimum to protect yourself

⇒ Most Countermeasures rely on Input for defining „normal“ Operation

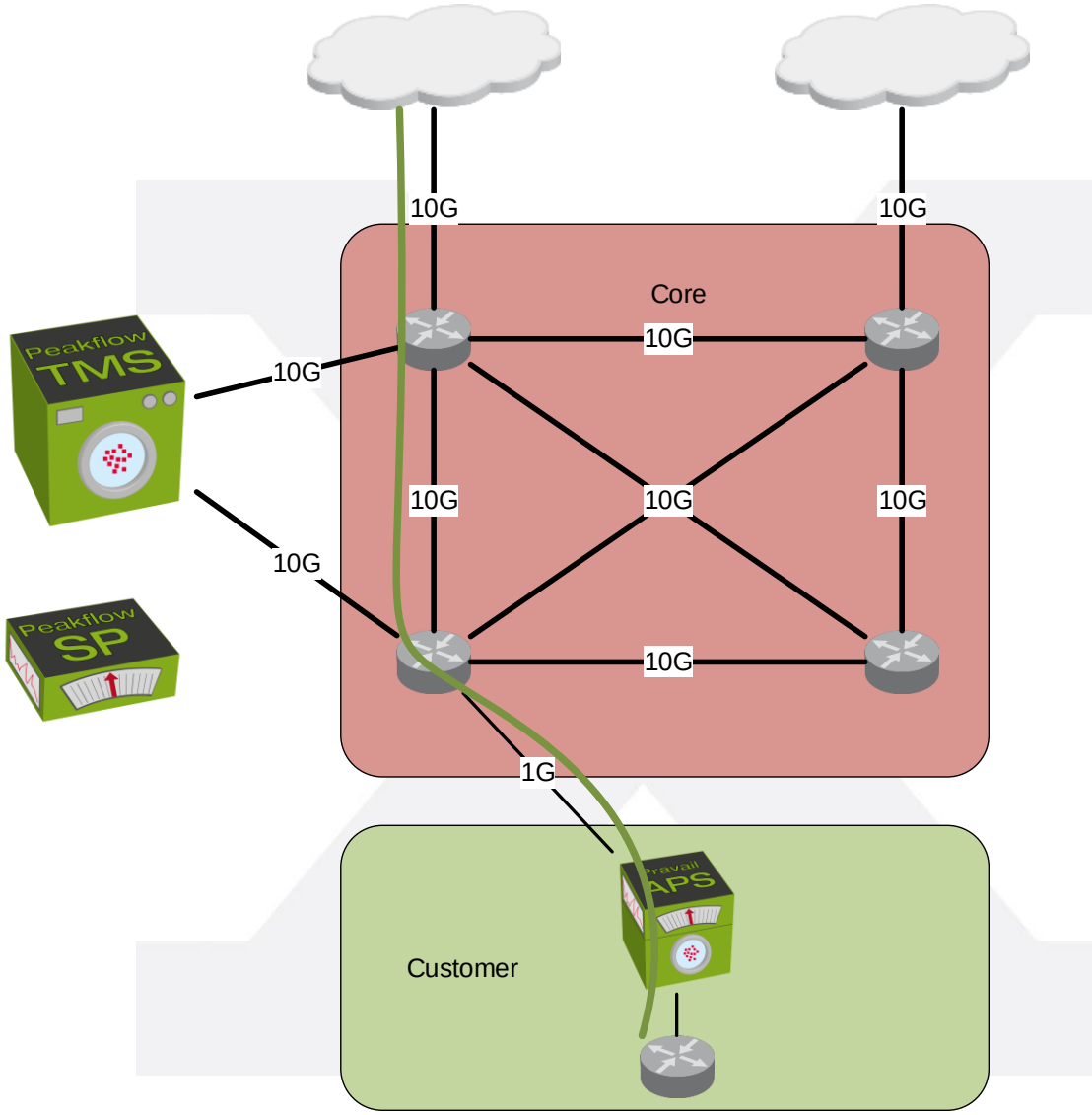
⇒ Only activate meaningful Countermeasures

Broaden your Defense

- Once identified as bad by Mitigation Appliance
  - If know bad source, block early
    - Blacklist on Mitigation Appliance hits before any expensive analysis is performed
    - Offload Blacklist to network ((s)RTBH, Flow Spec)
    - Share Knowledge (Fingerprints, Blacklists)
  - If only part of source is bad (e.g. 1/1000 Customers behind CGNAT)
    - Block Traffic but do NOT Blacklist
    - Identify Attacker and Share Knowledge
      - DDOS Sharing Initiative

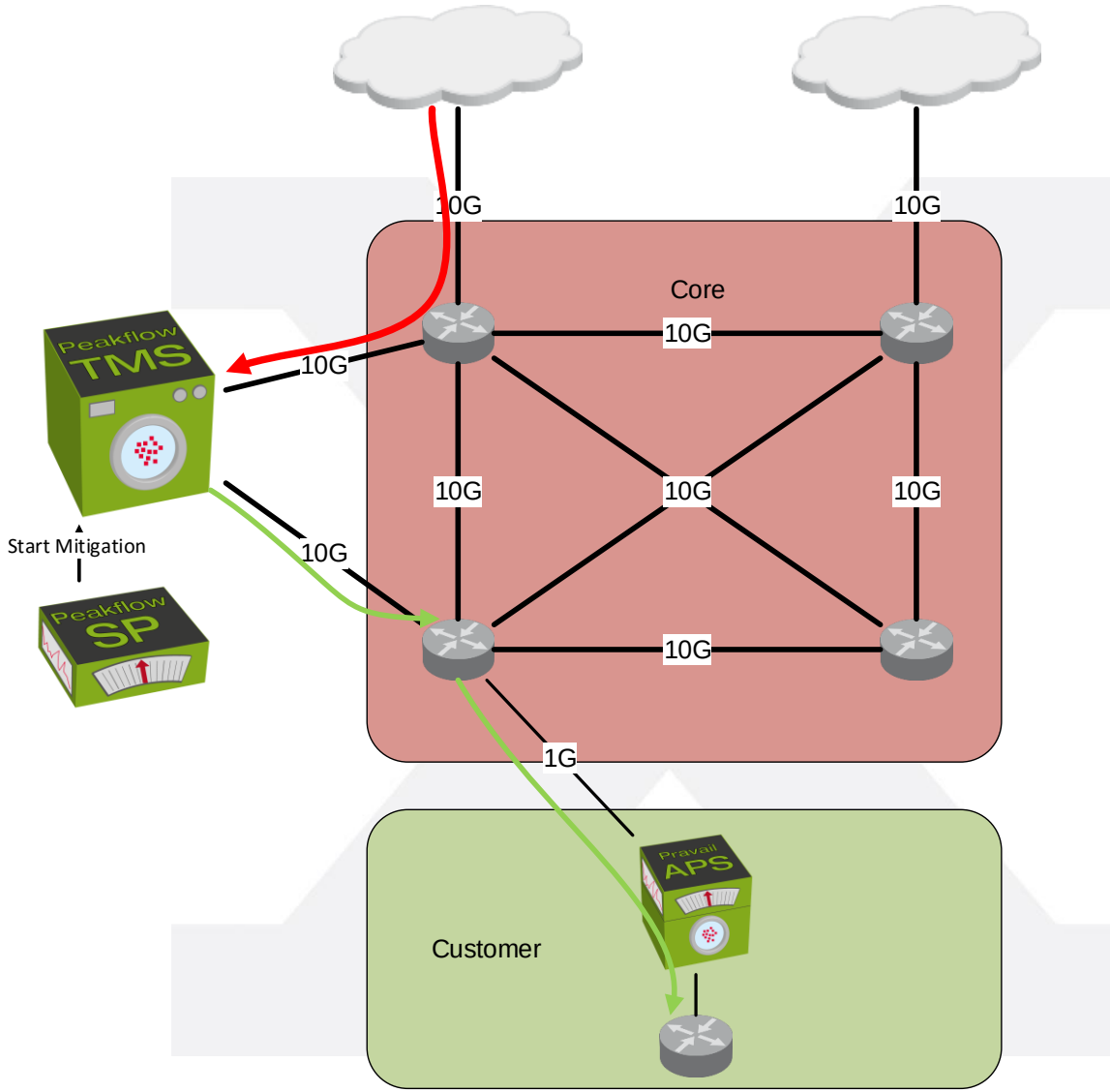
Normal Operation

- Core Router communicate with Peakflow SP
  - Core => SP send netflow/IPFIX
  - Core <=> SP speak BGP/SNMP
- Traffic passes Core Router
- Traffic passes APS
- Traffic reaches Customer Router



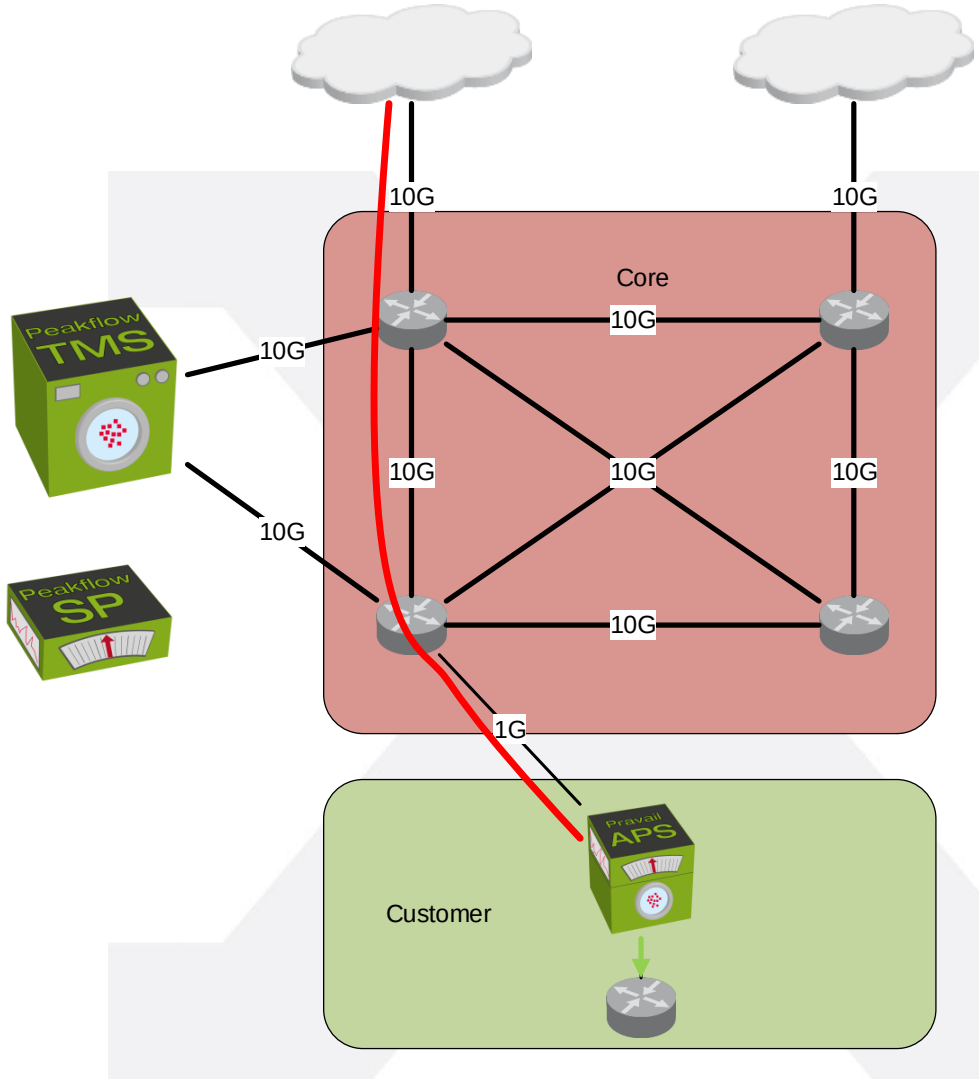
Volume Attack

- Peakflow SP detects Attack and raises Alarm
- Peakflow SP starts mitigation
  - Attack Traffic will be redirected to Peakflow TMS
  - PeakFlow TMS mitigates Attack
  - Peakflow TMS sends clean Traffic Back to Core
- Traffic passes APS
- Traffic reaches Customer Router



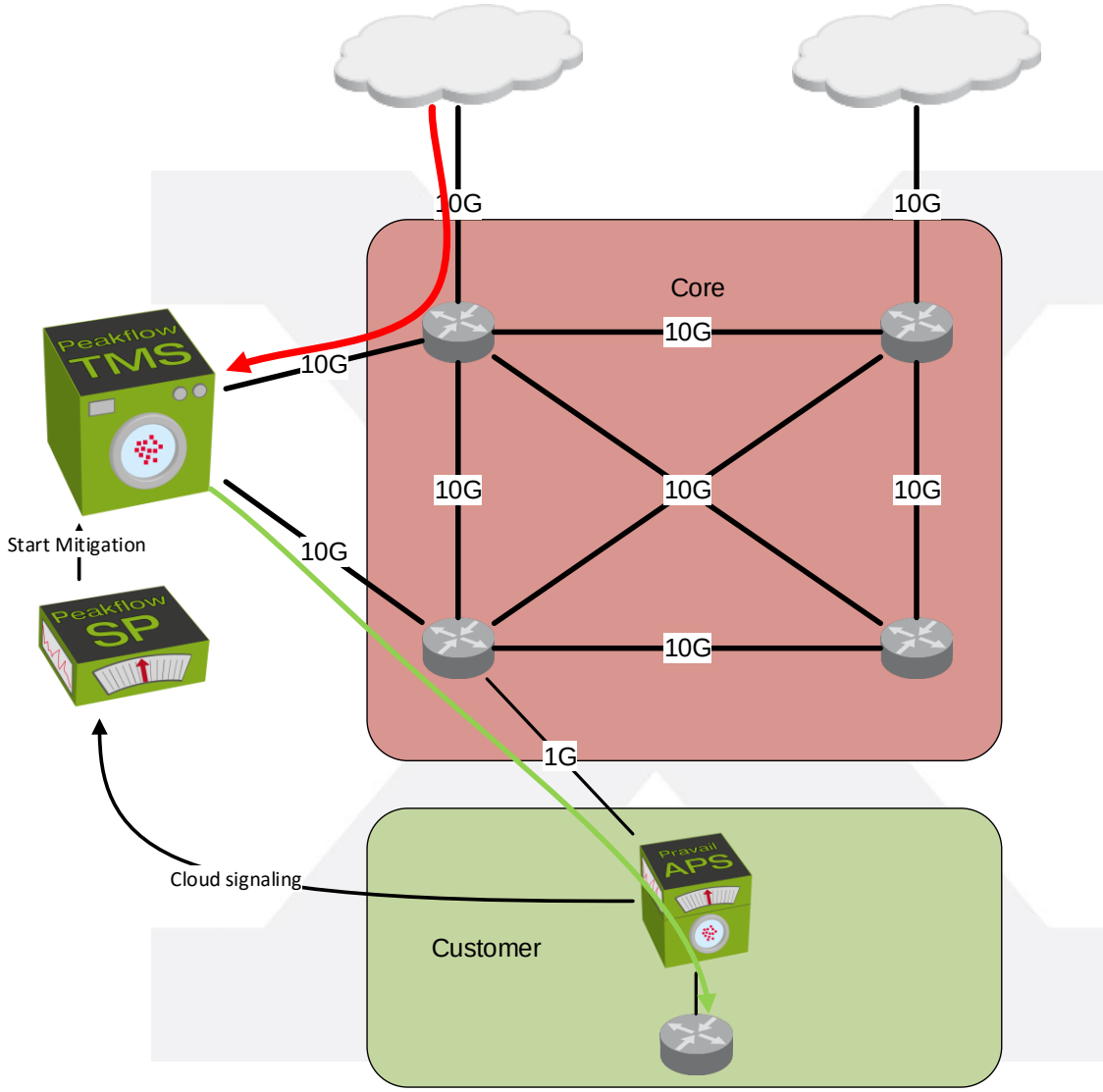
Small Attack

- Small Attack
  - low bandwidth (below 1G in this example)
  - Application based, thus not detectable via netflow
- Attack traffic passes Core router
- No alarm raised on Peakflow SP
  - Not detectable via netflow
- APS detects attack
- Attack traffic reaches APS
- APS mitigates attack traffic
- APS send clean traffic to customer



Larger Attack

- larger Attack
  - high bandwidth (above 1G in this example)
  - Application based, thus not detectable via netflow
- APS detects attack
  - local mitigation impossible due to bandwidth
- APS contacts Peakflow SP
  - uses cloud signalling
  - informs about attack type and size
- Peakflow SP starts mitigation
  - Attack Traffic will be redirected to Peakflow TMS
  - PeakFlow TMS mitigates Attack
  - Peakflow TMS sends clean Traffic to APS
- Clean Traffic passes APS



Market Players – Xantaro Partner Portfolio

Designing a Solution

- Integration of existing End to End Vendor Solution
  - Integrate into existing Network
  - Understand Traffic Flows
  - Deploy Solution
  - Support and Vendor Communication

- Create Xantaro Product
  - All of the above
  - Product Tailor made for Customer
  - Bring together vendors to form a solution