DDoS Protection in Backbone Networks
The Czech Way

Pavel Minarik, Chief Technology Officer
Holland Strikes Back, 3rd Oct 2017
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

1. Flow collection
2. DDoS detection
3. Routing control
4. Mitigation orchestration
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
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 …)
Response to Attack

- Alerting
  - E-mail, Syslog, SNMP trap

- Routing diversion
  - PBR (Policy Based Routing)
  - BGP (Border Gateway Protocol)
  - BGP Flowspec
  - RTBH (Remotely-Trigged 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

Internet Service Provider Core

Flow Data Collection
Learning Baselines

Anomaly Detection
Mitigation Enforcement

Traffic Diversion via
BGP Route Injection

Attack path
Clean path

Dynamic Protection
Policy Deployment
incl. baselines and
attack characteristics

Scrubbing center

Protected Object 1
e.g. Data Center,
Organization,
Service etc…

Protected Object 2

Service Provider Core

Internet
DDoS Protection Scenario 2
Mitigation with BGP Flowspec
BGP Flowspec

- 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
BGP Flowspec Scenario

Internet Service Provider Core

Flow Data Collection Learning Baselines

Anomaly Detection Mitigation Enforcement

Attack

Protected Object 1 e.g. Data Center, Organization, Service etc…

Protected Object 2

Sending specific Route advertisement via BGP FlowSpec

Dynamic signature:
- Dst IP: 1.1.1.1/32
- Dst Port: 135
- Protocol IP: 17 (UDP)
- Discard

Dropped traffic for
- Dst IP: 1.1.1.1/32
- Dst Port: 135
- Protocol IP: 17 (UDP)
Use Case: Carrier Grade Anti-DDoS
ČD Telematika AntiDDoS Service
ČD Telematika and its Core Infrastructure

**CORE CONNECTIVITY**
- 4x 10Gb/s NIX
- 3x10 Gb/s global transit
- 4x10Gb/s Google

**CONNECTED NETWORKS**
- 180+

**CONTRACTED TRAFFIC**
- 90 Gb/s

**REAL PEAK TRAFFIC**
- 50 Gb/s in
- 10Gb/s out
Why do we care about DDoS attacks on backbone?

- Attacks of multiple Gb/s hitting our customers
- No one is capable of handling volumes of Nx their port speed
- Cooperation with the ISP is a must
- Current solution based on filters and RTBH is insufficient
ČDT AntiDDoS Service

- Operated since July 2015
- Attack detection and re-routing with Flowmon DDoS Defender 40
- Scrubbing center for traffic “cleaning” is Radware DefensePro, 10Gbps of legitimate traffic + 12Gbps of attack
- Protection against volumetric attacks
ČDT-ANTI DDoS: Deployment scheme

Protected Objects e.g. Data Center, Organization, Service etc…

Access networks

Protected Objects e.g. Data Center, Organization, Service etc…

Access networks
A real customer case study

Local ISP – ČDT customer since 2007
1Gbps connectivity – no experience with attacks so far
A month of constant stream of attacks!
A real customer case study

706 different attacks, always multiple attacks in parallel

628
89% (628) attacks from multiple IPs

304
43% (304) attacks targeted multiple IPs

The Largest
The largest attack up to 19 Gbps (UDP flood)

The Longest
The longest lasting attack – 2:42h (DNS flood)
One month under attack

From internet to the scrubbing center

From the scrubbing center to the customer

Daily averages
ČDT-ANTIDDoS: Service options

- Normal path doesn’t go through the scrubbing center
- Attack detection by Flowmon
- Re-routing to the scrubbing center
- Attack mitigation starts within max 4 minutes since attack start

Traffic always goes through the scrubbing center
- Attack mitigation starts within max 1 minute since attack start

- Not under contract – activated by NOC on-demand
- Limited to 12 hours of scrubbing, max. 3x per annum

Always available

Always on

Emergency scrubbing
Automation

All the manual work is no longer necessary.

Entire process is fully automated, admins only receive a notification.

Speed

No need for human communication, alerting, process control.

Automated reporting for the attack start and end.

Reliability

In principle, nature of the deployment doesn’t leave a space for errors.

Benefits and Experience
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