Bandwidth Overload Avoidance using D-CAF

A Distributed, Context Aware Firewall

Cristián Varas, Thomas Hirsch

Fraunhofer FOKUS

Overview

- Background: Autonomic Networking
- Application: Overload avoidance
- Architecture
- Key Concepts
- Outlook: Context Valuation Framework

Fraunhofer FOKUS

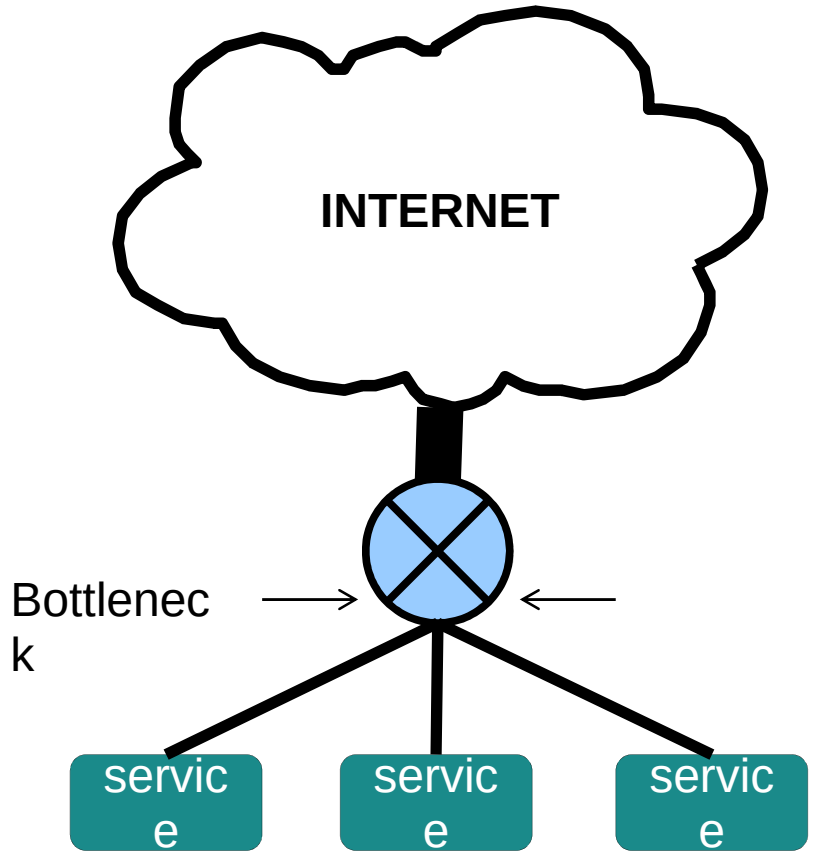
Autonomic Networking

- Computer Networks are growing ever more complex
- Self-Managing components need less configuration
  - They reconfigure to follow high-level policies
  - Autonomic nerve system: react without brain control
- Context Awareness allows local decisions and collaboration
  - Information is prepared by the specialized components
  - Exchange allows local decisions to follow global policies.

Fraunhofer FOKUS

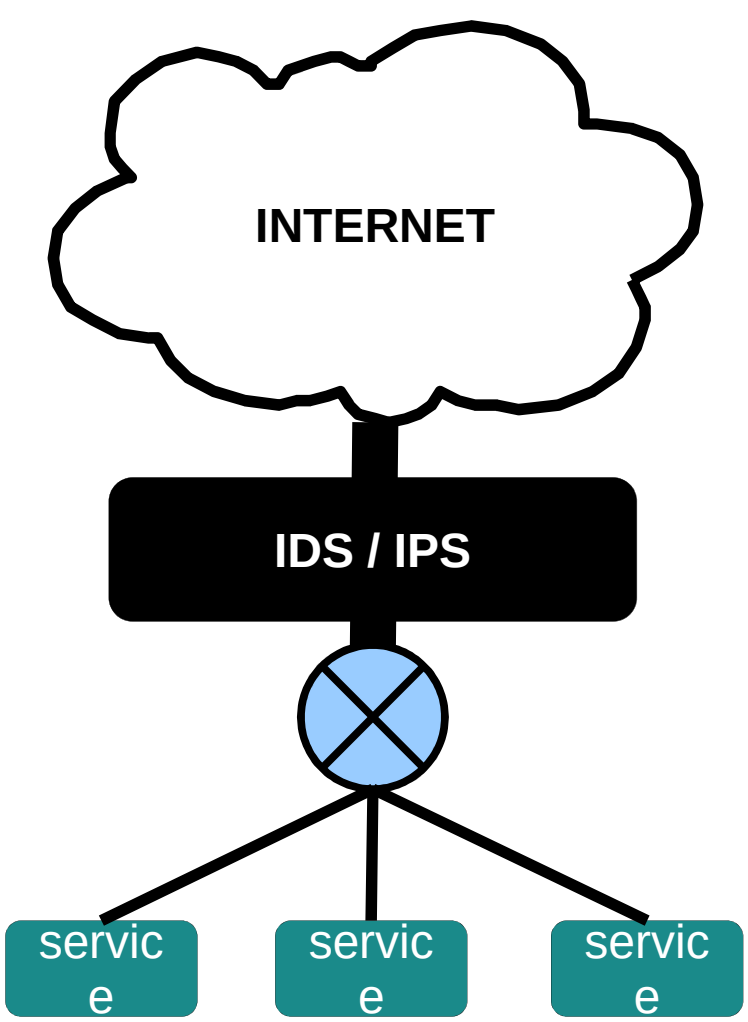
Application

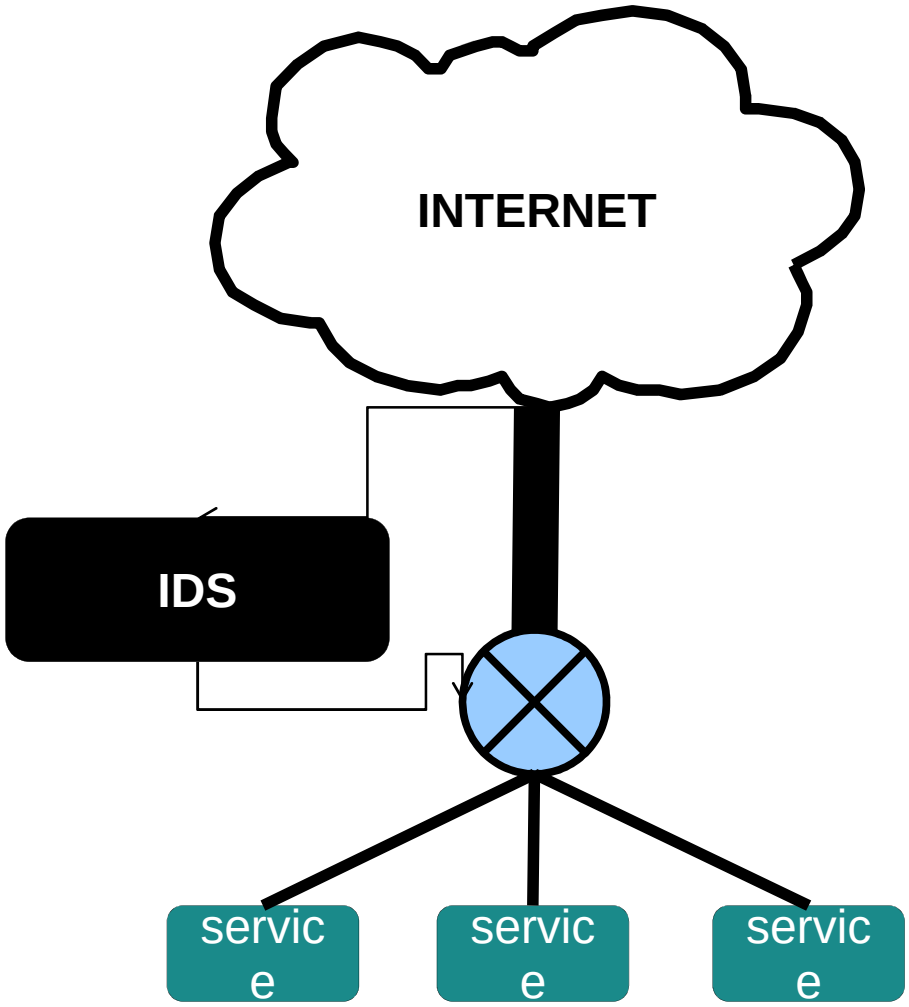
- Protection of network services (Firewall)
- Against abusive DDoS
- Against legitimate overload
  - (These do not actually differ)



Fraunhofer FOKUS

Conventional Solution



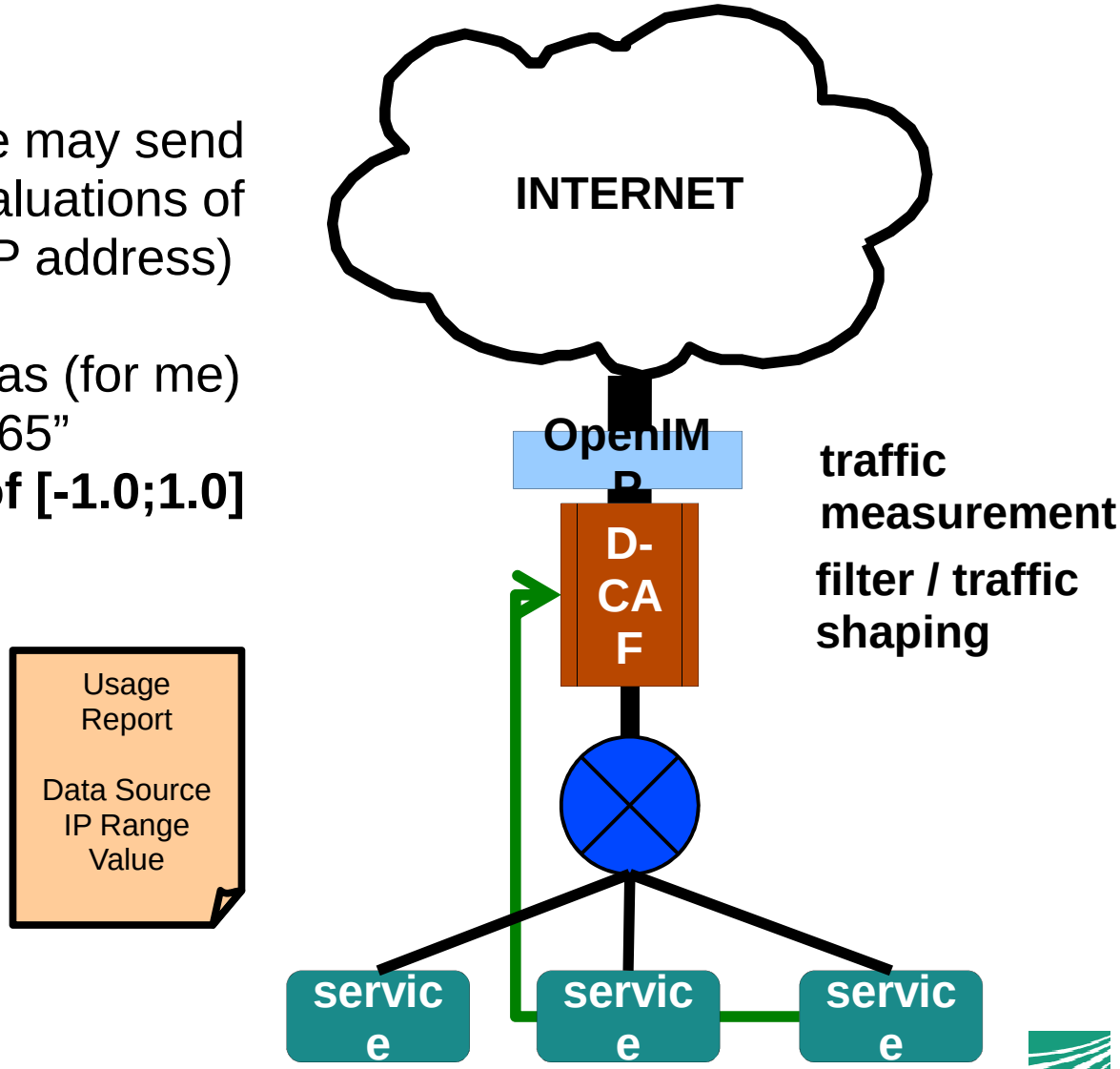


Fraunhofer FOKUS

Autonomic Approach: D-CAF

Each service may send subjective valuations of each user (IP address)

“IP 1.2.3.4 has (for me) a value of 0.65”
in a range of [-1.0;1.0]



Fraunhofer FOKUS

Autonomic Approach: D-CAF

- Services send subjective usage valuations of the users.
- The D-CAF system
  - collects these valuations
  - Monitors the total traffic, and traffic flows
- Only in case of overload, a decision has to be made:
  - We need to filter something to keep our services available
- The policy is to filter the worst valuated IP addresses
  - until the traffic is estimated to be within processable range.

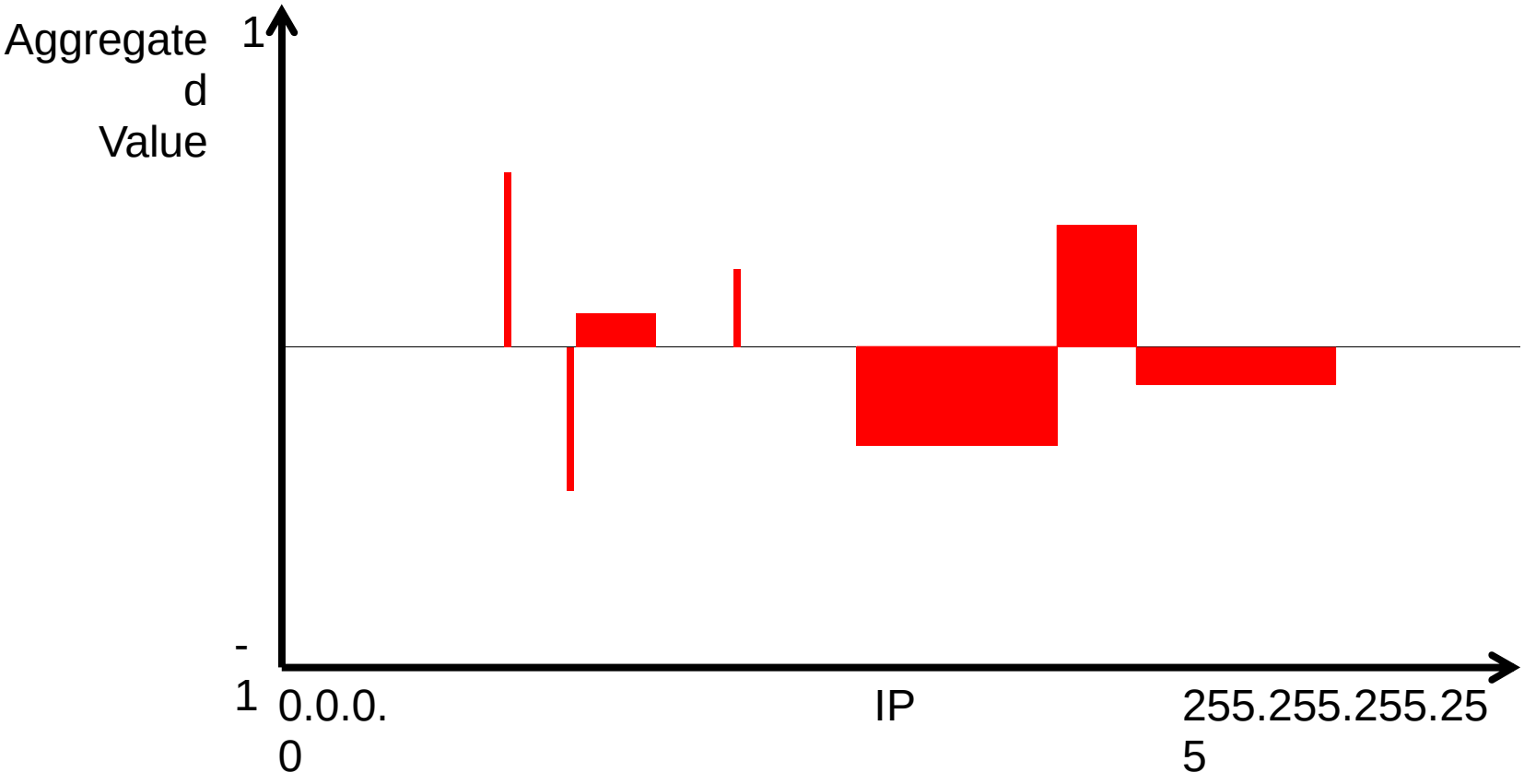
Fraunhofer FOKUS

Scenario: Normal usage

- Total traffic count < Available Bandwidth
  - Attack or not – we can handle it
- Services report usage valuations
  - User logged in with password → +0.8
  - Failed login attempt → -0.1
  - Regular browsing pattern → +0.5
  - Customer completed buying → +1.0
  - Repeatedly loading single site → -0.5
  - Attempt to log into database server → -0.9
  - ...

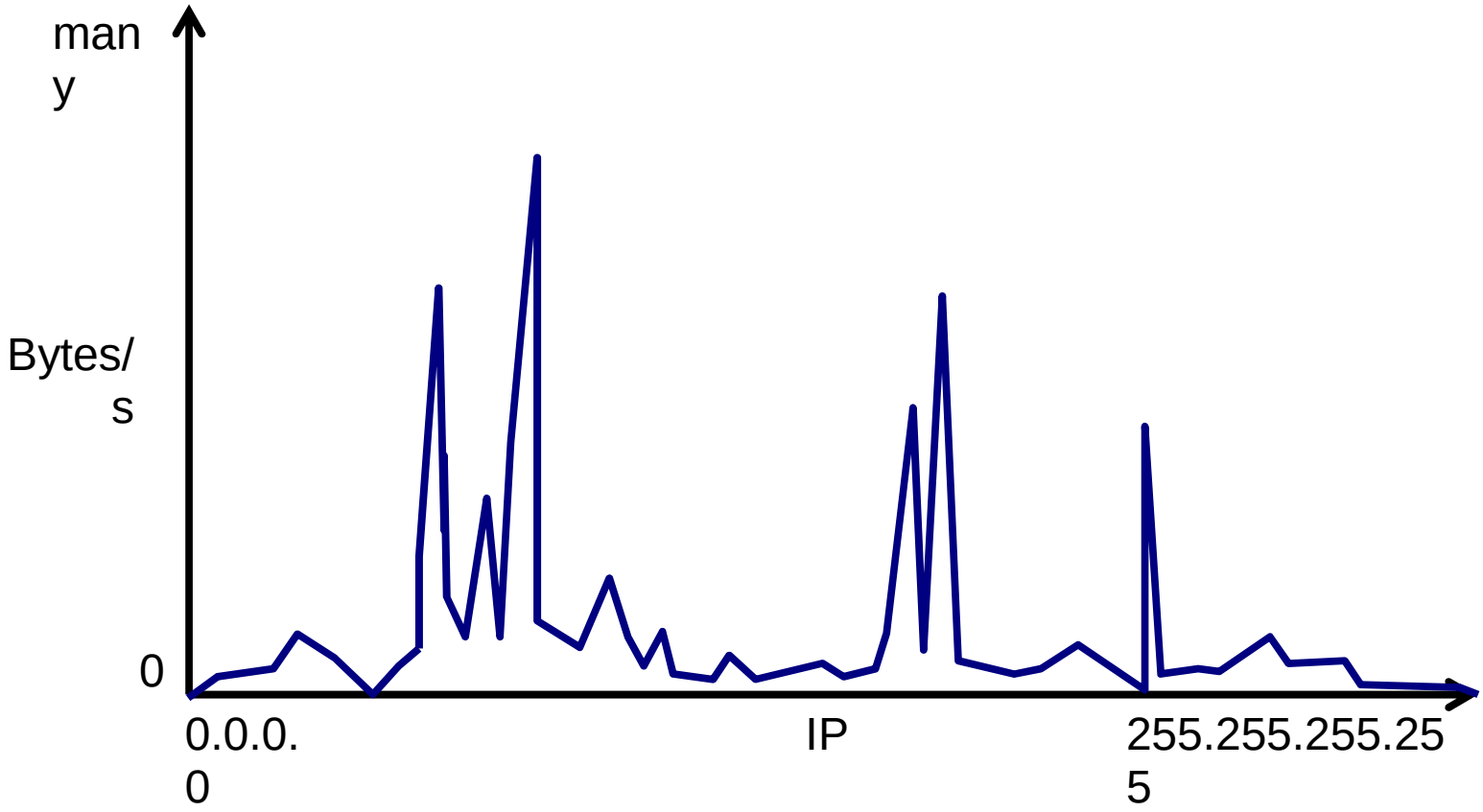
Fraunhofer FOKUS

Usage report aggregation



Fraunhofer FOKUS

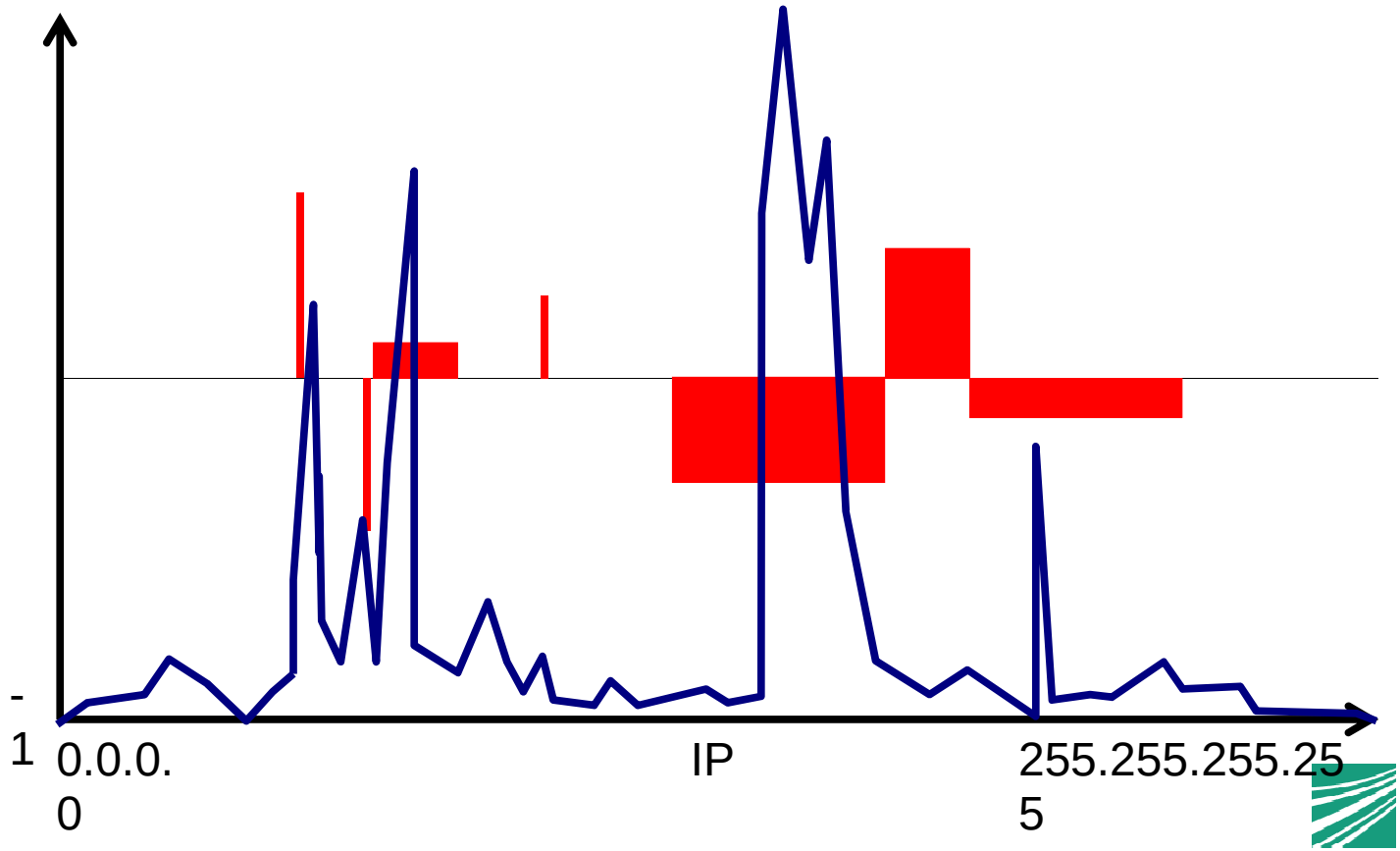
Per-Flow Traffic Measurement



Fraunhofer FOKUS

Scenario: Attack/Overload

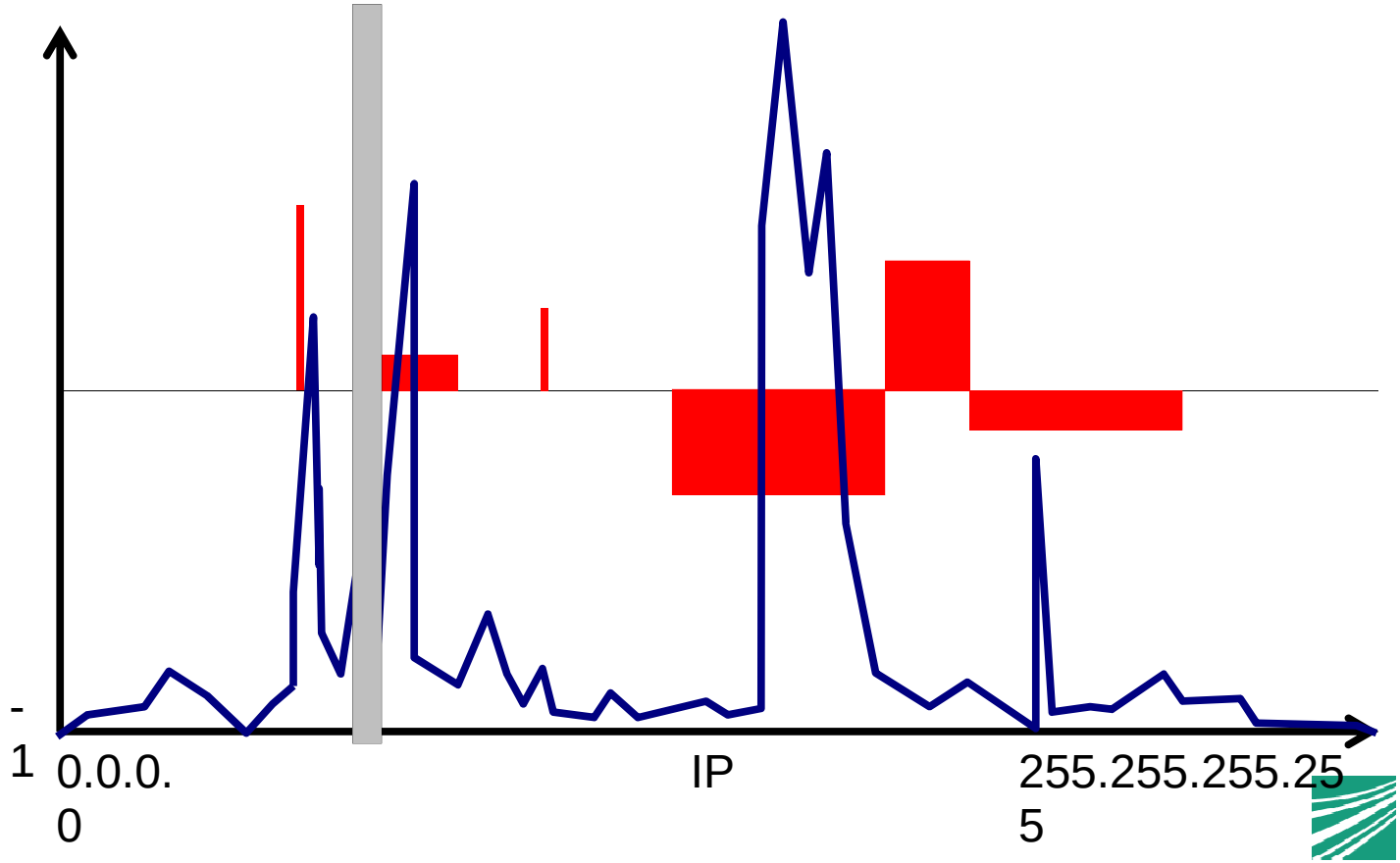
- Total traffic count >= Available Bandwidth
- We must filter – the least useful addresses first



Fraunhofer FOKUS

Scenario: Attack/Overload

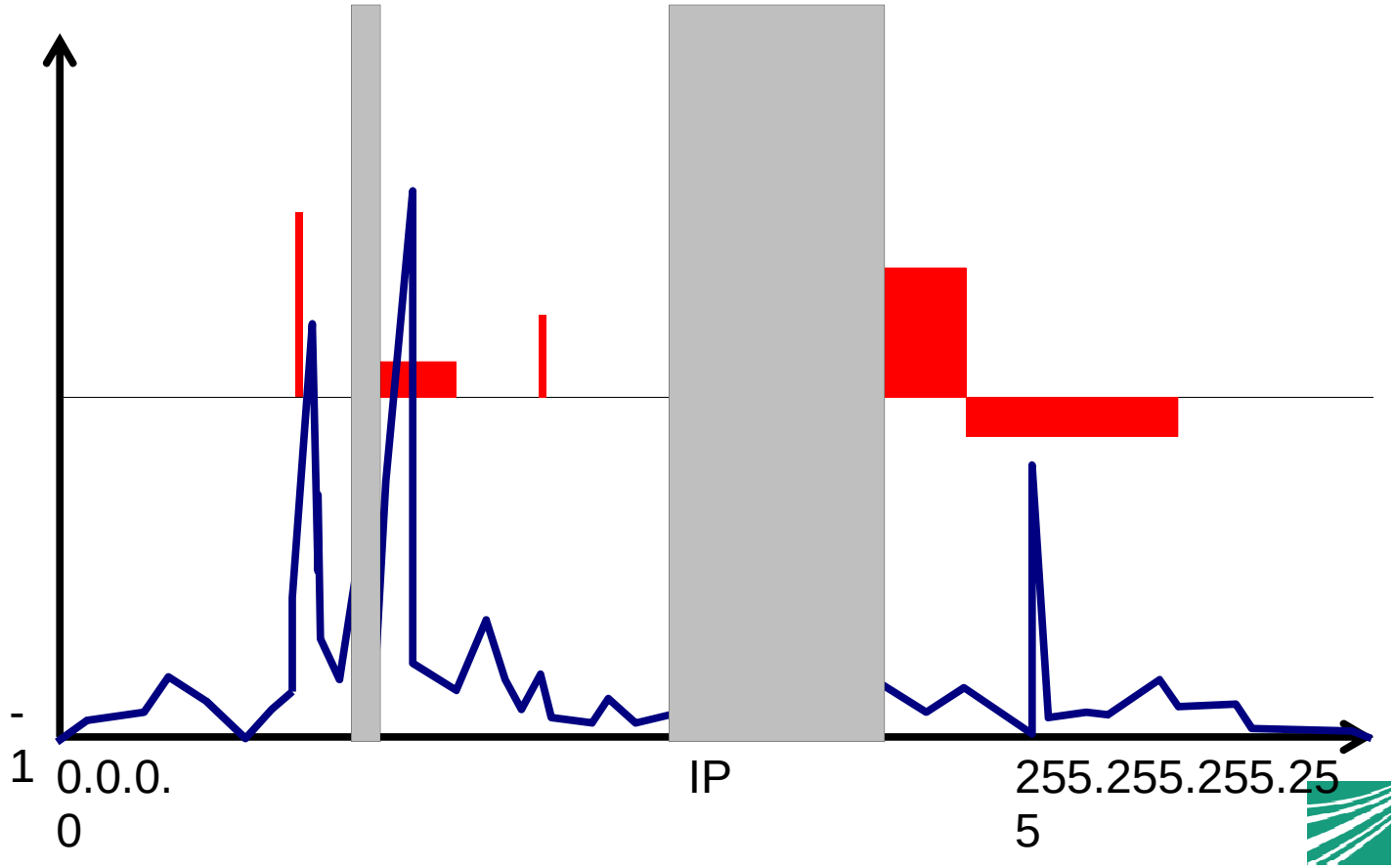
- Total traffic count still >= Available Bandwidth
- We must filter – the least useful addresses first



Fraunhofer FOKUS

Scenario: Attack/Overload

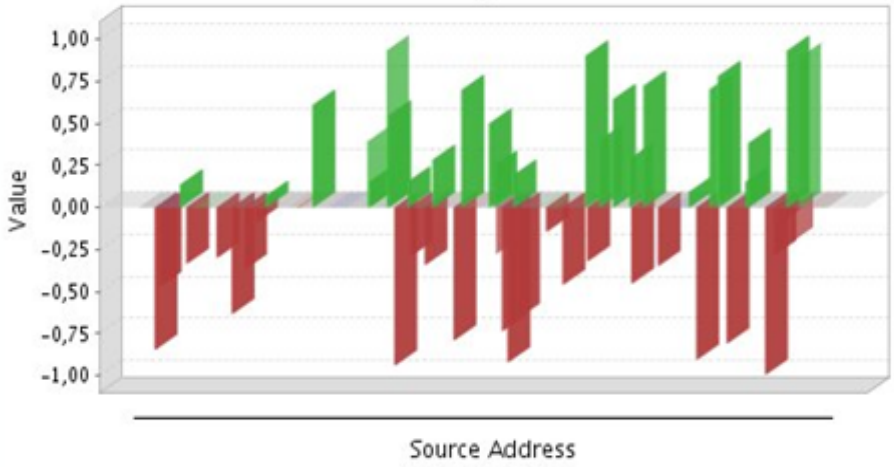
- Total traffic count < Available Bandwidth
- We have filtered enough



Fraunhofer FOKUS

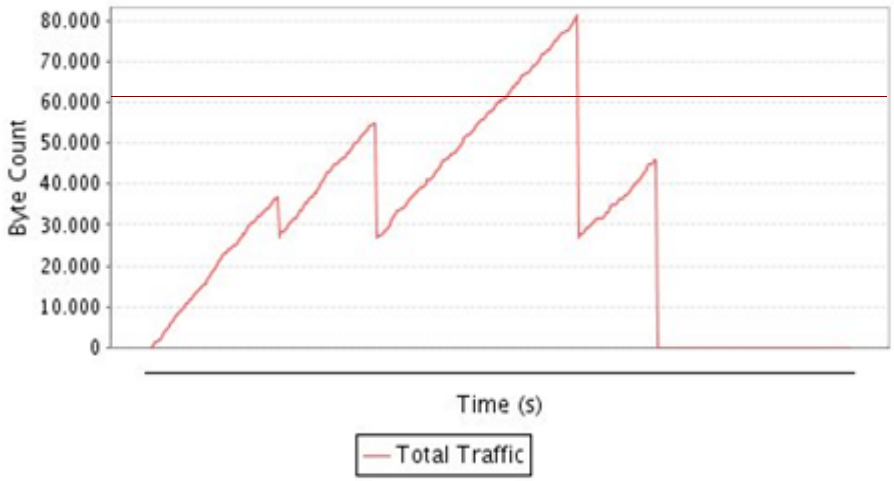
D-CAF: Distributed Context-Aware Firewall

Value by IP

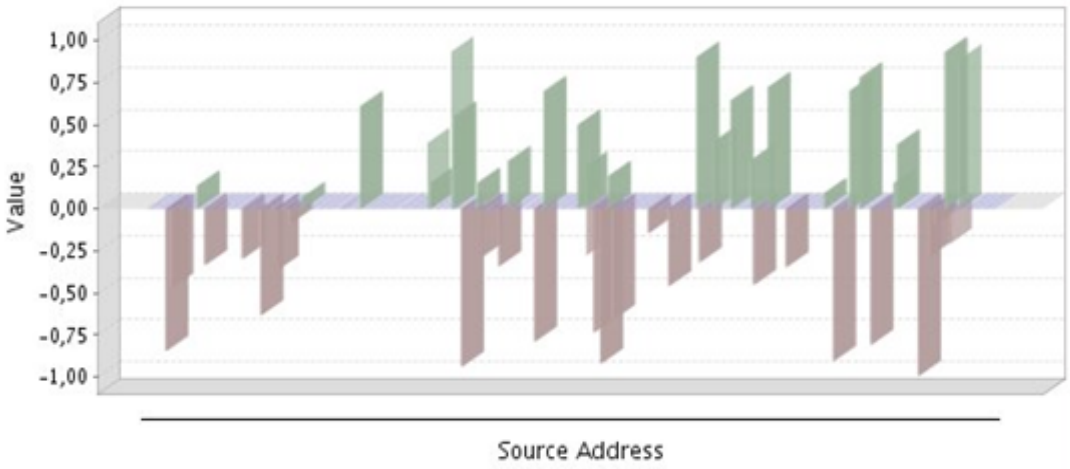


Traffic per Flow

Total Traffic



Filters



Received Packets : 92 Total Octetcount : 62856.0 Total Filters : 117

Threshold (KB/s): 123452 **Firewall Update Period (secs.):** 100 Apply

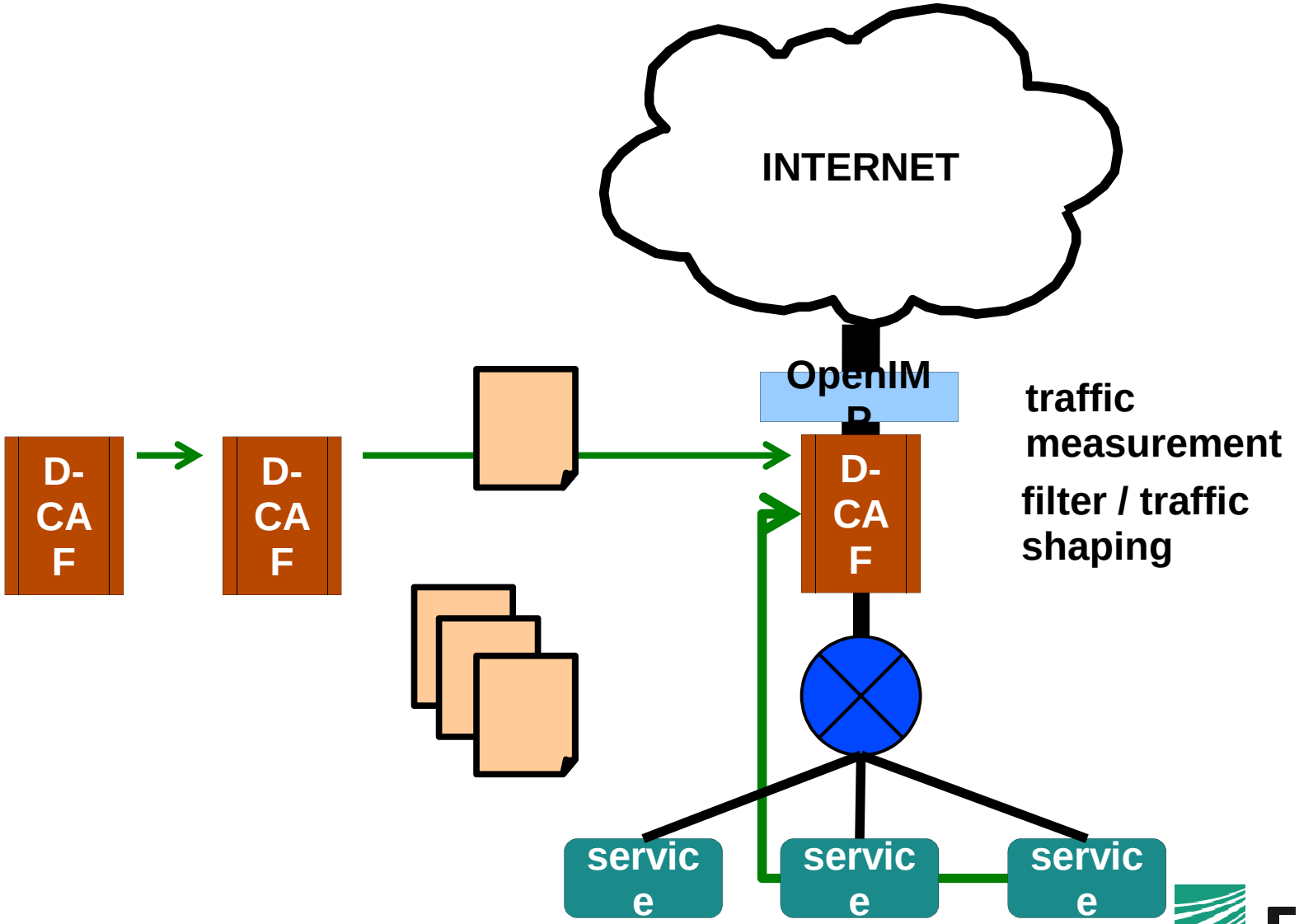
Fraunhofer FOKUS

Extending the context

- Valuation Reports are
  - Semantically concise; subjective
  - They can easily be exchanged in similar contexts
  - Just as well in aggregated form
  - “My neighbour thinks...”
- DDoS Attacks are
  - Distributed (zombies)
  - Highly similar (simple)
  - Using same resources (infected hosts)

Fraunhofer FOKUS

Extending the context



Fraunhofer
FOKUS

Outlook

- Currently tested: Single instance DDoS defense
  - Setup a larger distributed reporting network
  - e.g. in the Onelab2 distributed testbed

In Autonomic Networking

- Can be extended to other contexts:
  - IP address = identification = UserID; ServiceID; ...
  - Traffic/Value = Cost/Value = universal
- Generalization: Context Valuation Framework

Fraunhofer FOKUS

Thank you!

- Questions? -

Cristián Varas, Thomas Hirsch

cristian.varas@fokus.fraunhofer.de
thomas.hirsch@fokus.fraunhofer.de

Fraunhofer FOKUS