



# DDoS - FoD

## DDoS Mitigation Tool

**GEANT Information & Infrastructure Security Team**

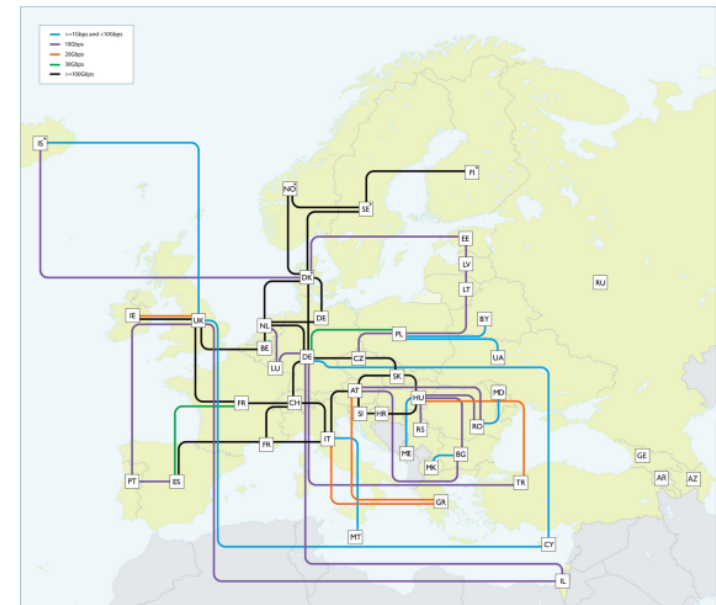
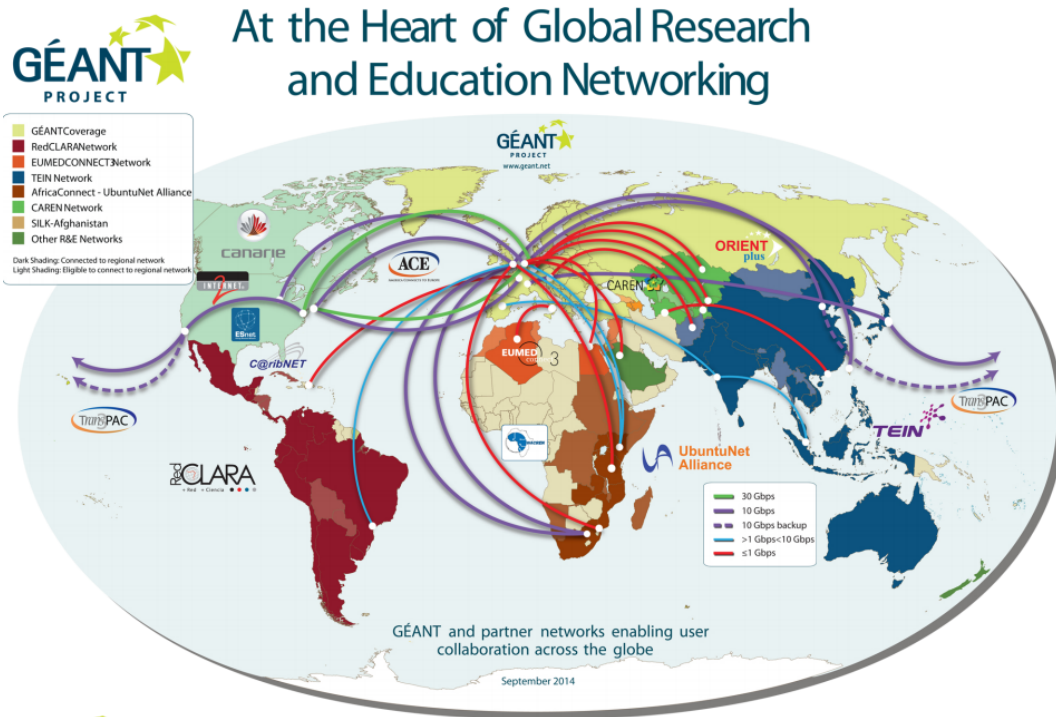
Evangelos Spatharas

CEE Peering Days

Budapest, March 30<sup>th</sup> 2016



# Who is GÉANT?

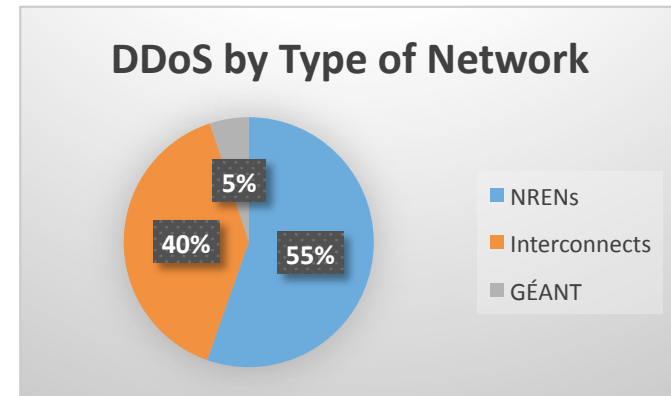
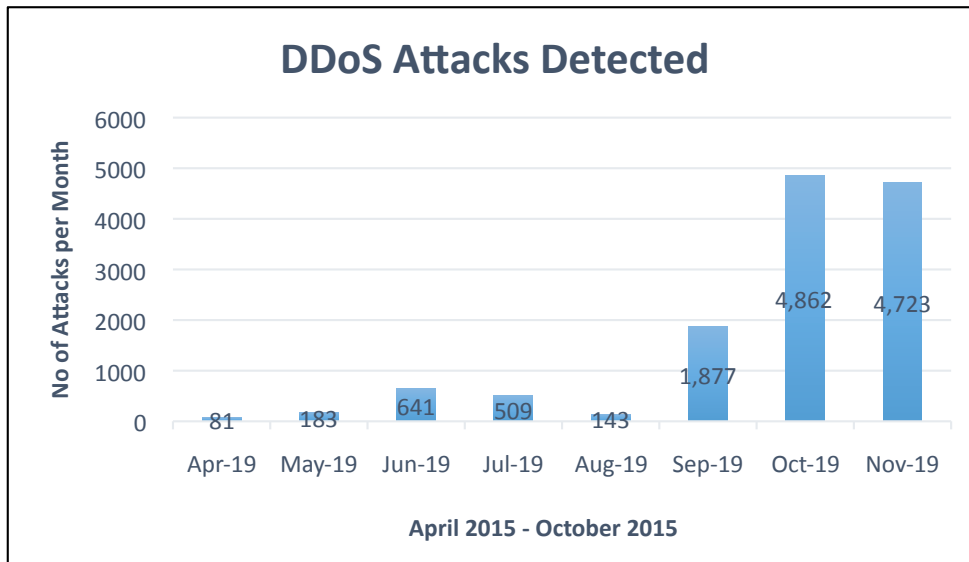


GÉANT connectivity as at January 2014.



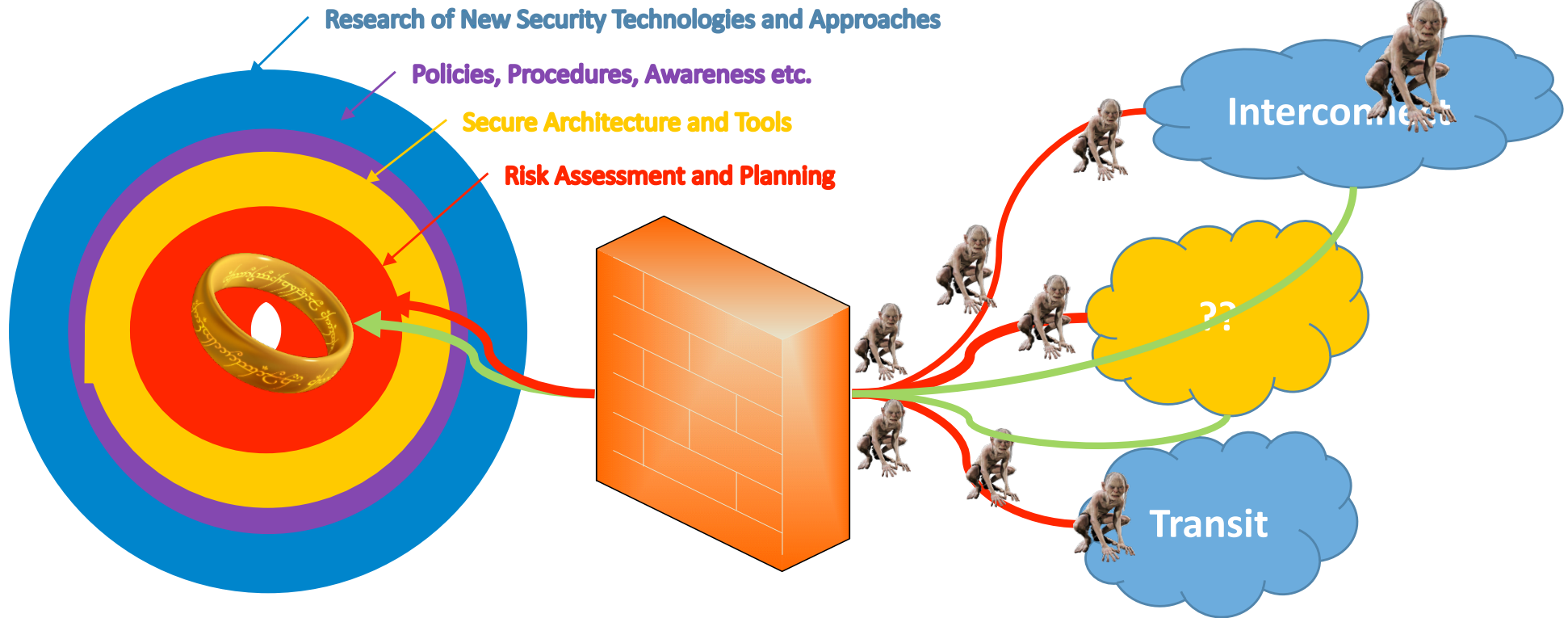
# Network Attacks

## GÉANT

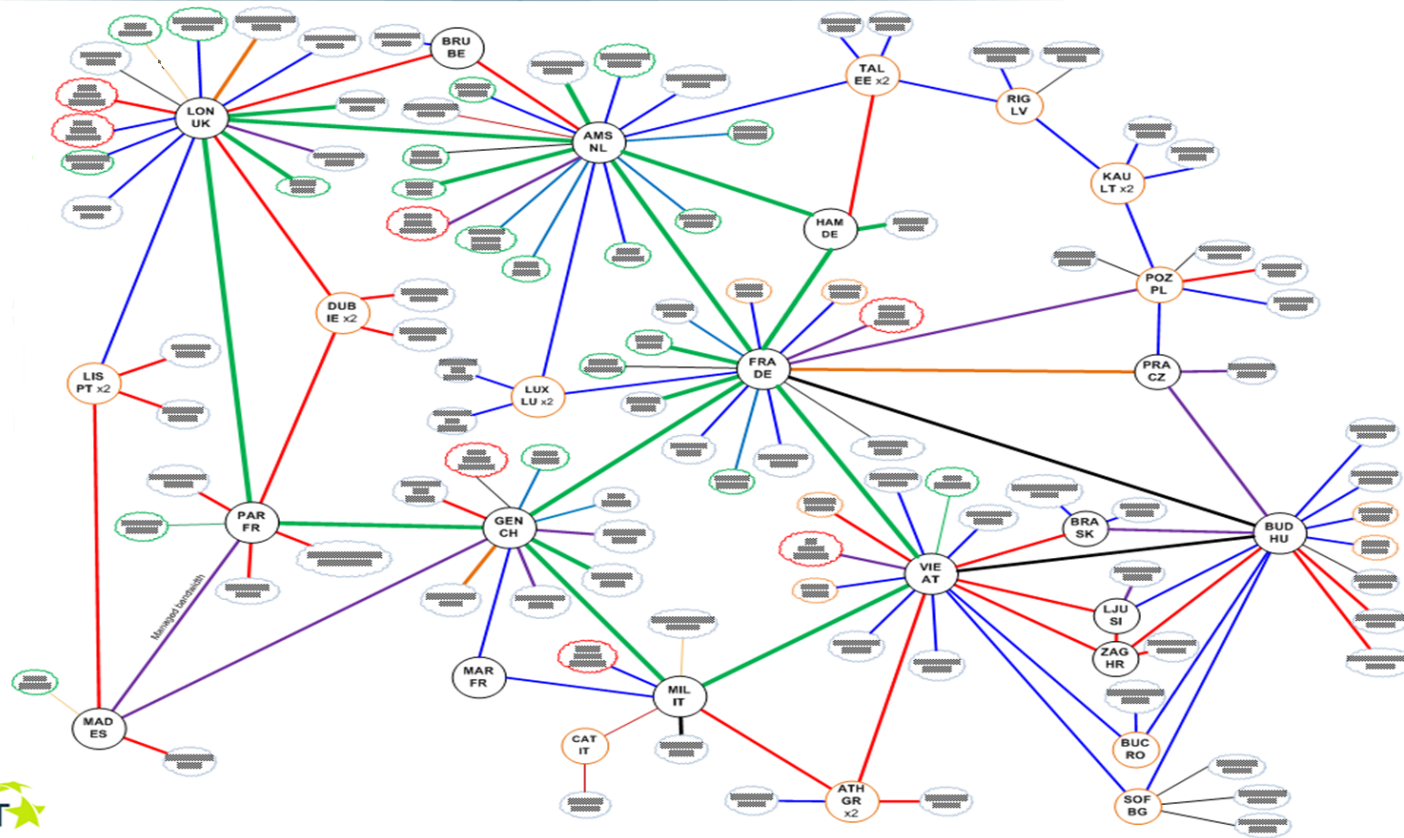


DNS, NTP, SMTP and other amplification attacks..

# GÉANT's Security Approach



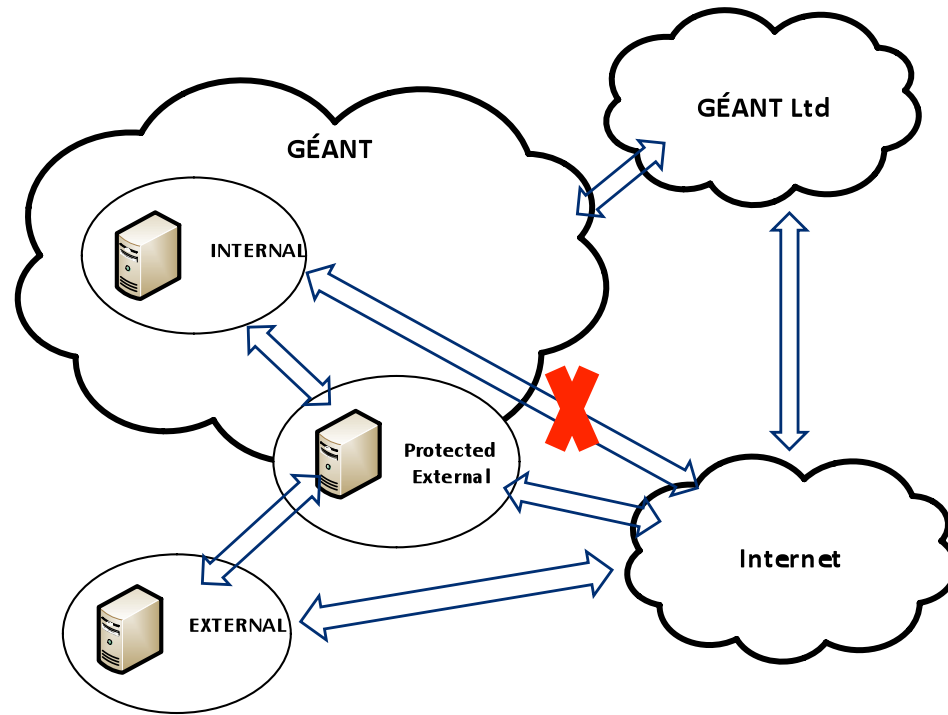
# Defending GÉANT



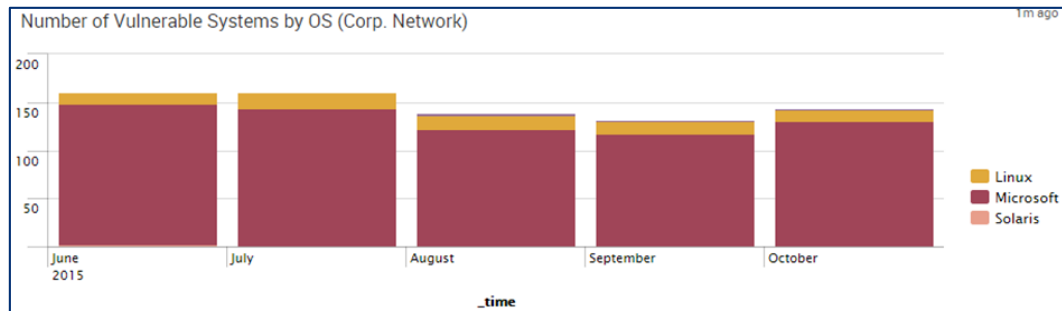
## Defending GÉANT



# Preventative Controls - Zones



## Preventative Controls – Others



### Number of Vulnerable System by OS

- Asset management
- Areas of attention
- Monthly scans

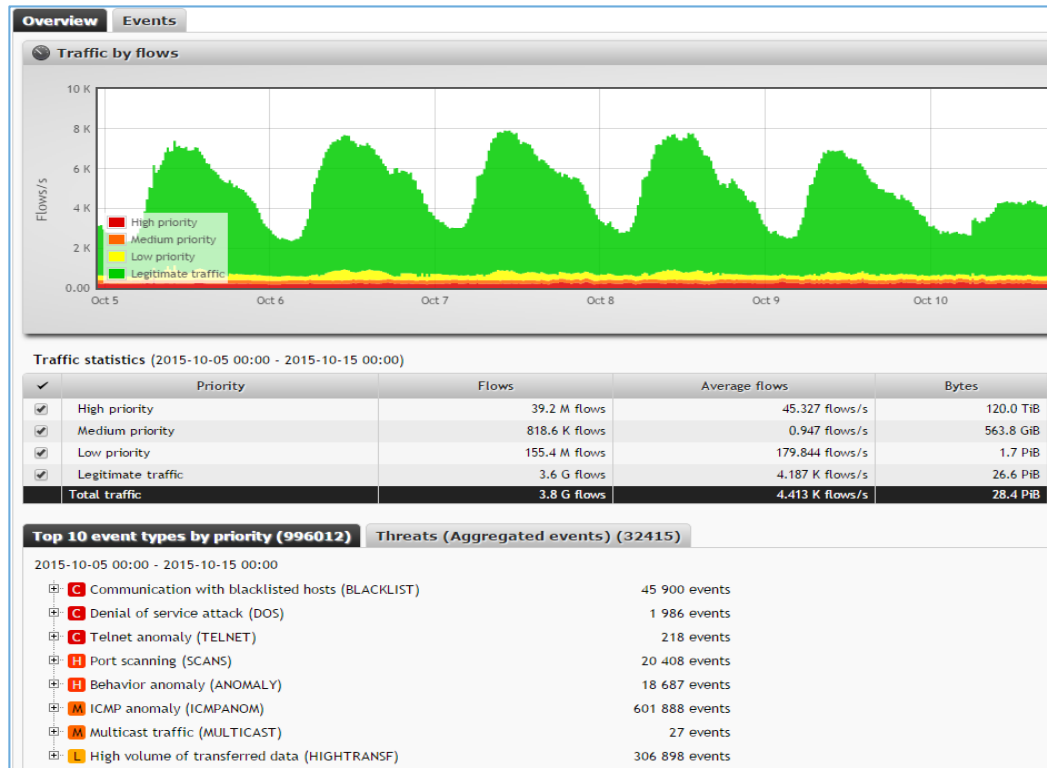
### Others

- uRPF
- Bogons
- Spoofing
- Etc










# NetFlow Monitoring + ADS



## FlowMon

- NetFlow v9
- 33 Juniper MXs
- > 900M flows per day
- 1:100 sampling rate
- Entry points
- Fan-out for other tools
- Not just anomaly detection tool
- Alerts
- Redundancy?
- Many methods..

# NetFlow Alerts + Automated Tickets = NSHaRP

CRITICAL 	HIGH 	MEDIUM 	LOW 	INFORMATION 
ANOMALY		HTTPDICT		
DOS				
RDPDICT				
SSHDICT				
TELNET				

- Based on criticality
- Per client basis
- Automatic closure
- Mainly an NREN service
- Daily reports



```

Dear NREN,

We have detected a Communication with blacklisted hosts event affecting your network. All
the information pertaining to it can be found below:

=====
#Start Time: 2015-10-30 00:22:11 UTC
#Protocol: TCP
#Source IP: ██████████.110.30
#Target IPs: ██████████.52.61
#Ports: 56118

#Evidence:
Source IP;Source port;Destination IP;Destination
port;Protocol;Timestamp;Duration;Transferred;Packets;Flags;Source AS;Destination AS
██████████.110.30;80;██████████.52.61;56118;TCP;2015-10-30
00:22:11.419;0;2840000;2000;.A....;██████████;██████████

=====

If you wish to reply to this email please leave the subject unaltered so the ticket can be
updated accordingly.

If no response is received, this ticket will be automatically closed after 5 working days

Regards,

GEANT CERT
cert@oc.geant.net (PGP Key ID: 99833085 / Fingerprint: 3CBF F211 8305 635D 5839 BB27 BA6B
F34A 9983 3085)
Phone no.: +44 (0)1223 866 140
  
```

## Mitigation



## ACLs– Chain Architecture

```

[redacted]@[redacted]re0> show configuration interfaces ge-0/2/0.210
description "SRV_GLOBAL INFRASTRUCTURE VLAN210 | Test security alerting software | CONTACT:IT@geant.org  IMPLEMENTED:20150714";
vlan-id 210;
family inet {
  filter {
    input-list [ PROTECTED_EXTERNAL_HEAD_IN VL210_MIDDLE_IN PROTECTED_EXTERNAL_TAIL_IN ];
    output-list [ PROTECTED_EXTERNAL_HEAD_OUT VL210_MIDDLE_OUT PROTECTED_EXTERNAL_TAIL_OUT ];
  }
  address 62.40.[redacted];
}
family inet6 {
  filter {
    input-list [ PROTECTED_EXTERNAL_V6_HEAD_IN VL210_V6_MIDDLE_IN PROTECTED_EXTERNAL_V6_TAIL_IN ];
    output-list [ PROTECTED_EXTERNAL_V6_HEAD_OUT VL210_V6_MIDDLE_OUT PROTECTED_EXTERNAL_V6_TAIL_OUT ];
  }
  address 2001:798:[redacted];
}

```

### Chain architecture

- Head → Middle → Tail
- Auditing
- Troubleshooting
- Deployment

## RTBH

```
@mx1.vie.at.re0> show route community 20965:0008
inet.0: 557244 destinations, 2424476 routes (557168 active, 12 holddown, 193 hidden)
+ = Active Route, - = Last Active, * = Both

144.64/32 * [BGP/170] 36w1d 16:17:06, localpref 100, from 62.40.
AS path: I, validation-state: unverified
> to 192.0.2.101 via dsc.0
179.255/32 * [BGP/170] 3w1d 15:11:53, localpref 200, from 62.40.
AS path: 2108 ?, validation-state: unverified
> to 192.0.2.101 via dsc.0
180.25/32 * [BGP/170] 4w3d 18:38:48, localpref 200, from 62.40.
AS path: 2200 I, validation-state: unverified
> to 192.0.2.101 via dsc.0
[BGP/170] 5w5d 14:37:08, localpref 200, from 62.40.
AS path: 2200 I, validation-state: unverified
> to 192.0.2.101 via dsc.0
243.59/32 * [BGP/170] 1d 21:19:46, localpref 200, from 62.40.
AS path: 2108 ?, validation-state: unverified
> to 192.0.2.101 via dsc.0
243.158/32 * [BGP/170] 1d 21:20:16, localpref 200, from 62.40.
AS path: 2108 ?, validation-state: unverified
> to 192.0.2.101 via dsc.0
218.101/32 * [BGP/170] 3d 00:21:49, localpref 200, from 62.40.
AS path: 2847 51172 I, validation-state: unverified
> to 192.0.2.101 via dsc.0
[BGP/170] 3d 00:21:49, localpref 200, from 62.40.
AS path: 2847 51172 I, validation-state: unverified
> to 192.0.2.101 via dsc.0

evangelos@mx1.vie.at.re0> show firewall filter RTBH-count
Filter: RTBH-count
Counters:
Name Bytes Packets
RTBH-count 2010285515822 2955402767
```

### Statistics

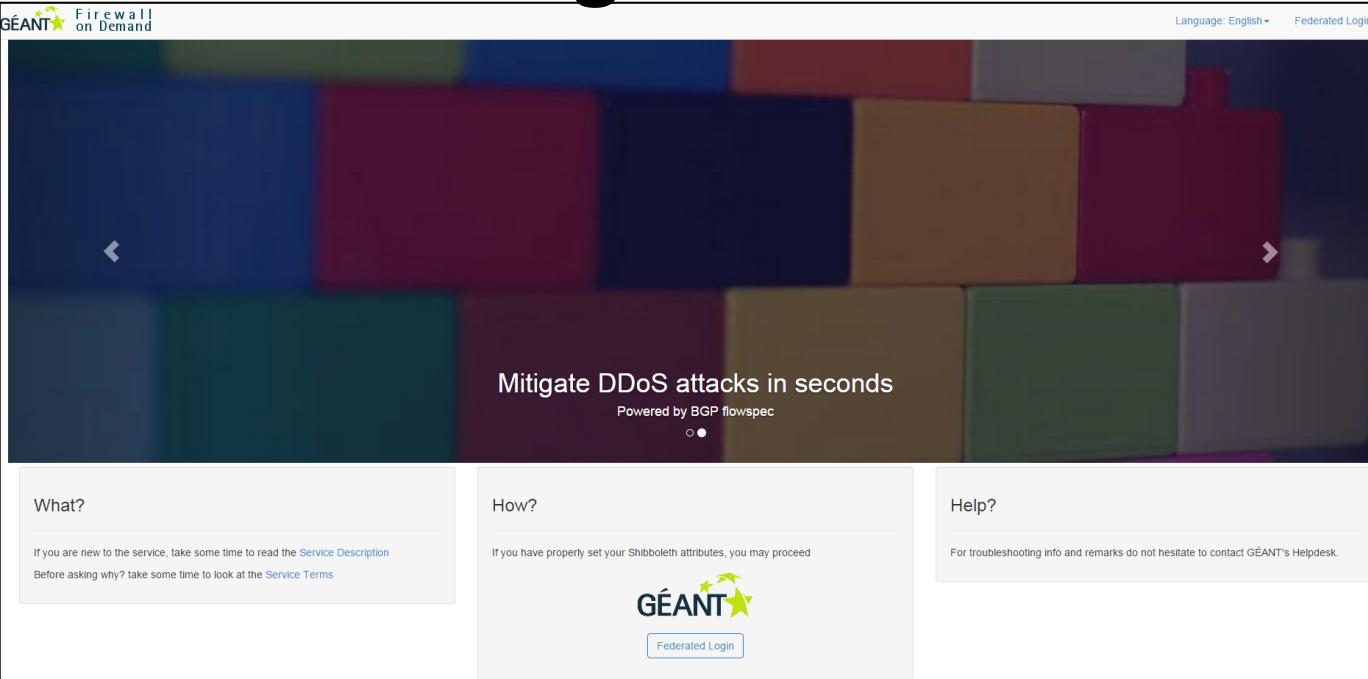
- 6 RTBH-ed destinations
- ~3 billions of packets blocked

Counters reset every week!!


### Other

- UTRS service – Team CYMRU
- Cogent RTBH service
- Etc.

# fod.geant.net



The screenshot shows the homepage of the 'fod.geant.net' service. At the top left, it says 'GÉANT Firewall on Demand'. At the top right, there are links for 'Language: English' and 'Federated Login'. The main banner features a dark background with colorful, abstract rectangular blocks and the text 'Mitigate DDoS attacks in seconds' followed by 'Powered by BGP flowspec'. Below the banner are three columns of information:

- What?**  
If you are new to the service, take some time to read the [Service Description](#)  
Before asking why? take some time to look at the [Service Terms](#)
- How?**  
If you have properly set your Shibboleth attributes, you may proceed  
  
[Federated Login](#)
- Help?**  
For troubleshooting info and remarks do not hesitate to contact GÉANT's Helpdesk.

# FoD WEB GUI

Firewall Rule

- [Dashboard](#)
- [Rules](#)
- [Add Rule](#)
- [Overview](#)
- [Admin](#)
- [My profile](#)

## My rules

Firewall Rules

records per page

ACTIVE
PENDING
ERROR
DEACTIVATED

Search:

[Previous](#)
1
[Next](#)

Showing 1 to 4 of 4 entries

Name	Match	Then	Status	Applier	Expires	Response	Actions
SSH_DISCARD_20150815_S2JEK7	Dst Addr █████ 0.2/32 Src Addr 0.0.0.0/0 Protocols tcp DstPorts 22	discard	ACTIVE	fod (GEANT)	2015-08-22	Successfully committed	<a href="#">Edit</a> <a href="#">Deactivate</a>
NTP_DISCARD_20150816_G6MLVL	Dst Addr █████ 0.7/32 Src Addr 0.0.0.0/0 Protocols udp DstPorts 123	discard	ACTIVE	fod (GEANT)	2015-08-24	Successfully committed	<a href="#">Edit</a> <a href="#">Deactivate</a>
RDP_DISCARD_20150819_BJFYR5	Dst Addr █████ 0.6/32 Src Addr 0.0.0.0/0 Protocols tcp DstPorts 3389	discard	ACTIVE	fod (GEANT)	2015-08-24	Successfully committed	<a href="#">Edit</a> <a href="#">Deactivate</a>

free to include any additional comments.

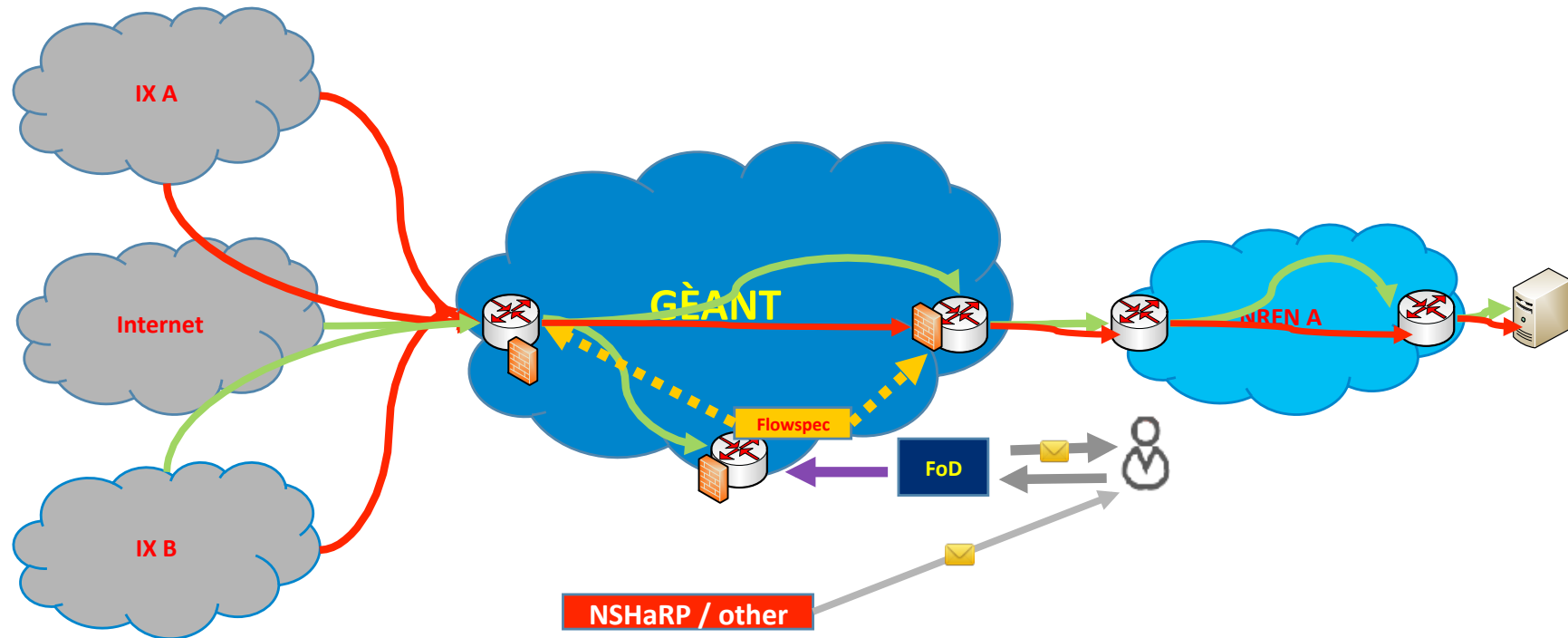


## Demo Time!

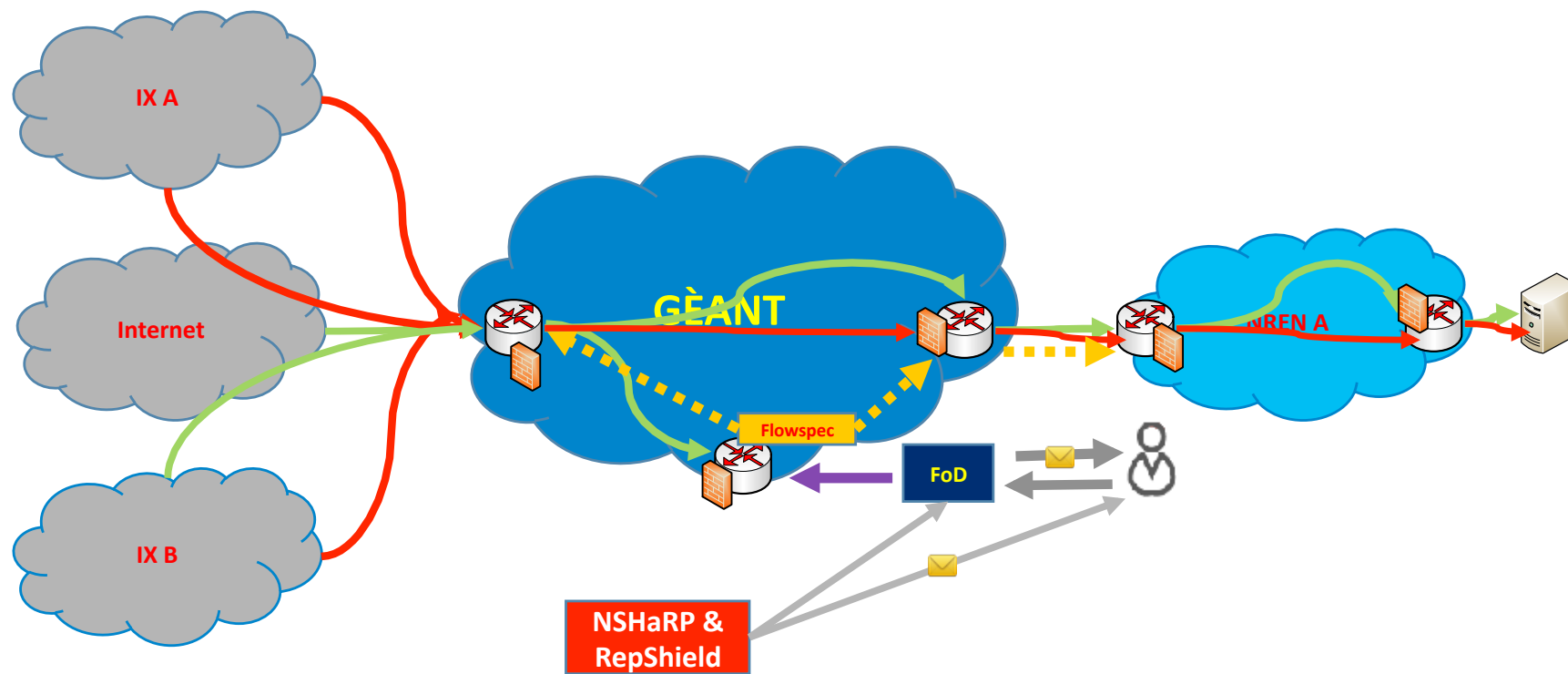
---



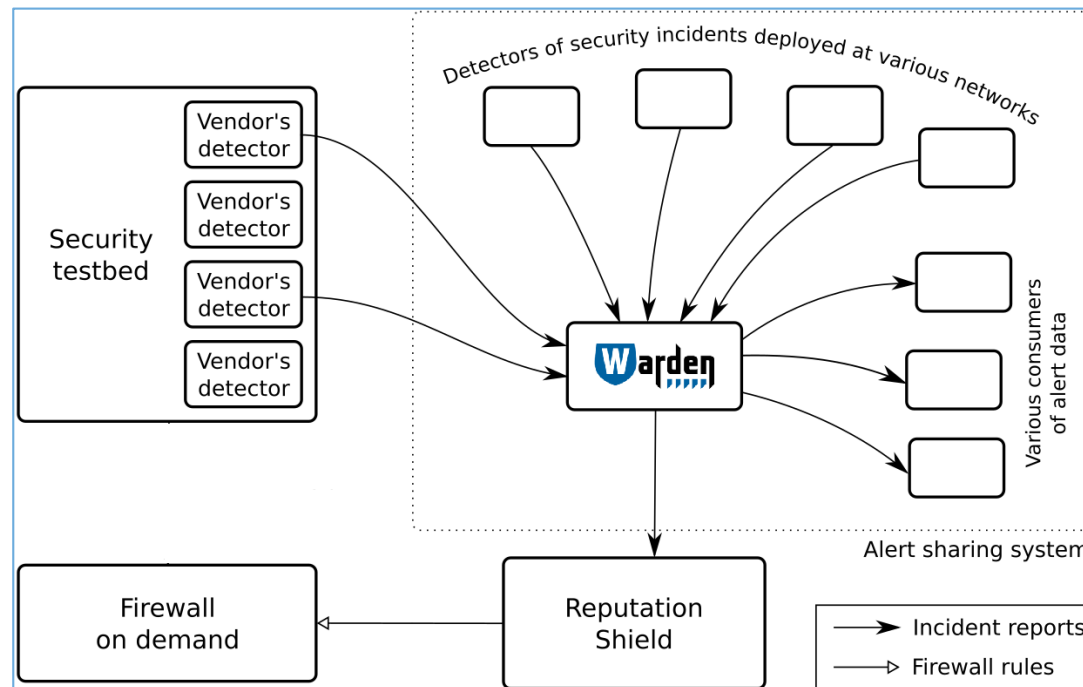
## Under the hood – Current Status



# Upgrade – Future Plans



# Lessons Learned



## What do YOU think?

---

What do YOU think?



## Q & A

---





Thank you

GEANT Information & Infrastructure Security Team

[Evangelos.Spatharas@geant.org](mailto:Evangelos.Spatharas@geant.org)



Networks · Services · People  
[www.geant.org](http://www.geant.org)