

GÉANT Perspective on DDoS

DDoS Mitigation in the NREN Environment Workshop

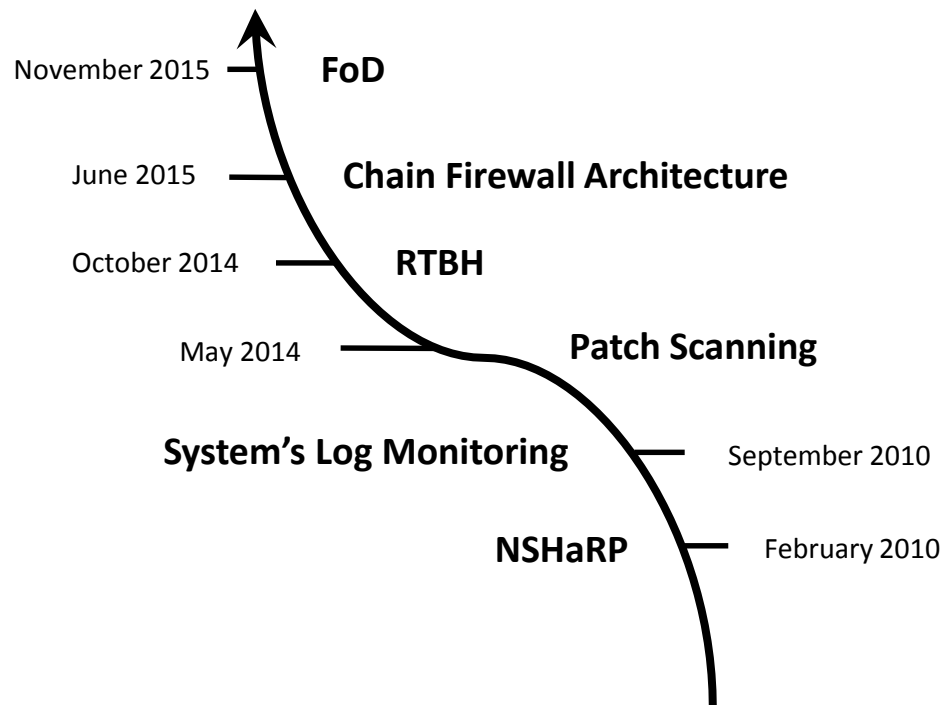
GEANT Information & Infrastructure Security Team

Evangelos Spatharas

DDoS Mitigation Workshop

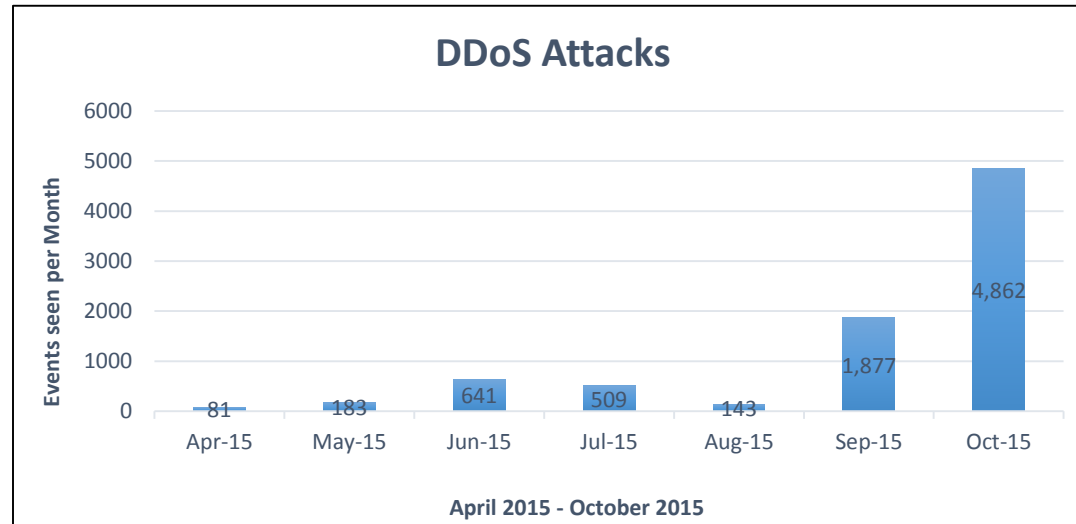
Vienna, November 10th 2015

- DDoS
 - Statistics
- How to Prevent
 - Understand your Network
 - Network Architecture - Zones
 - Modular Firewall
- How to Detect
 - NetFlow Monitoring and Alerting
 - NetFlow Alternatives – Log Monitoring
- How to Mitigate
 - ACLs
 - RTBH
 - BGP Flowspec
- The Future of BGP Flowspec
 - Firewall on Demand
 - NSHaRP Fully Integration
- Q & A



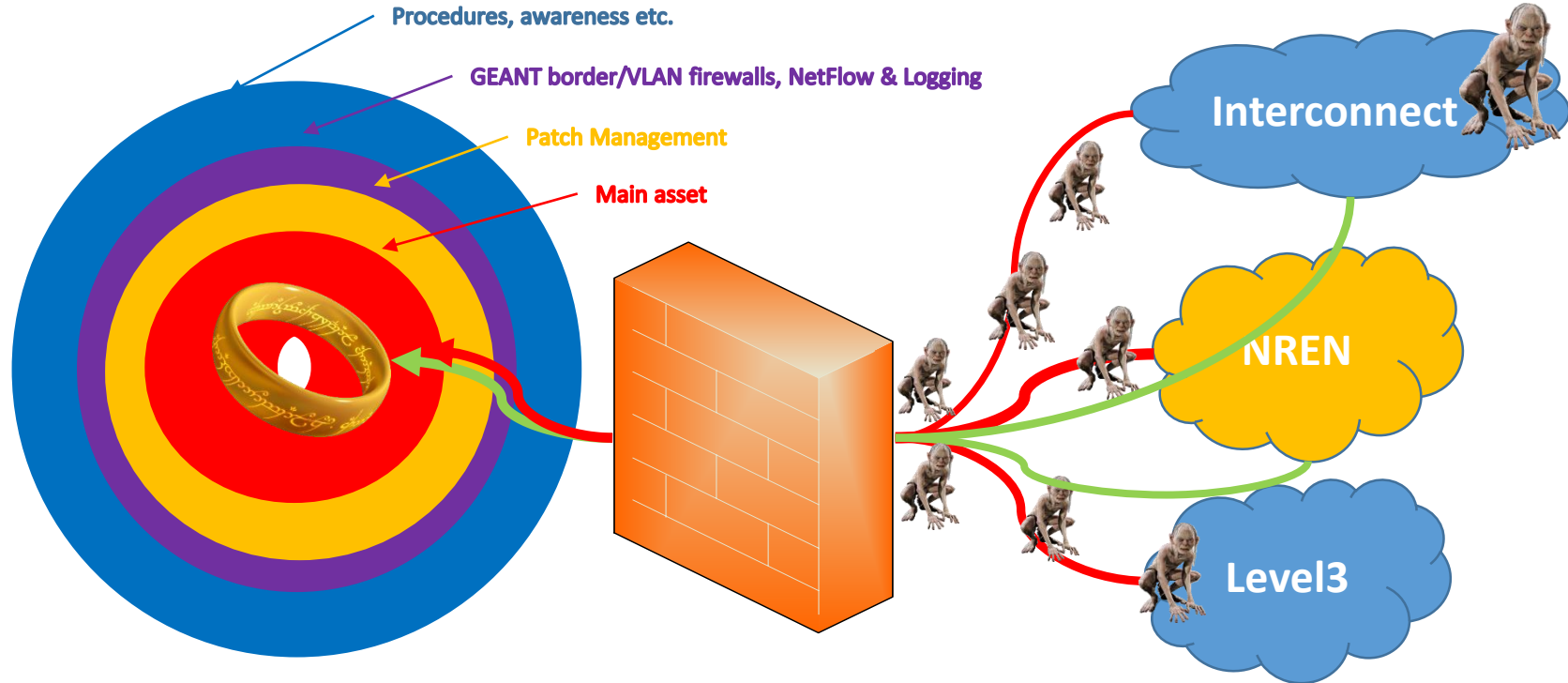
D(D)oS – Not Just in Fiction Movies

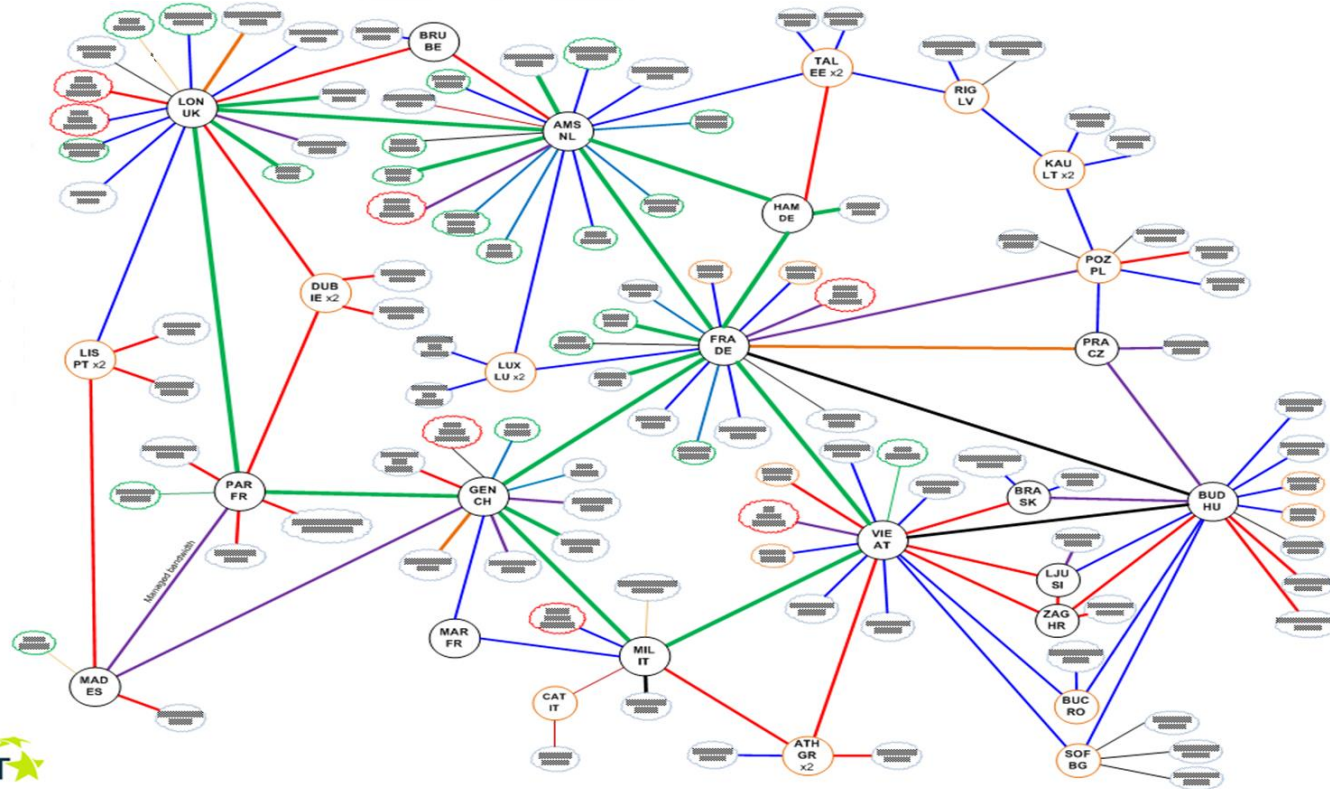
GÉANT



- DNS, NTP, SMPT and other amplification attacks..

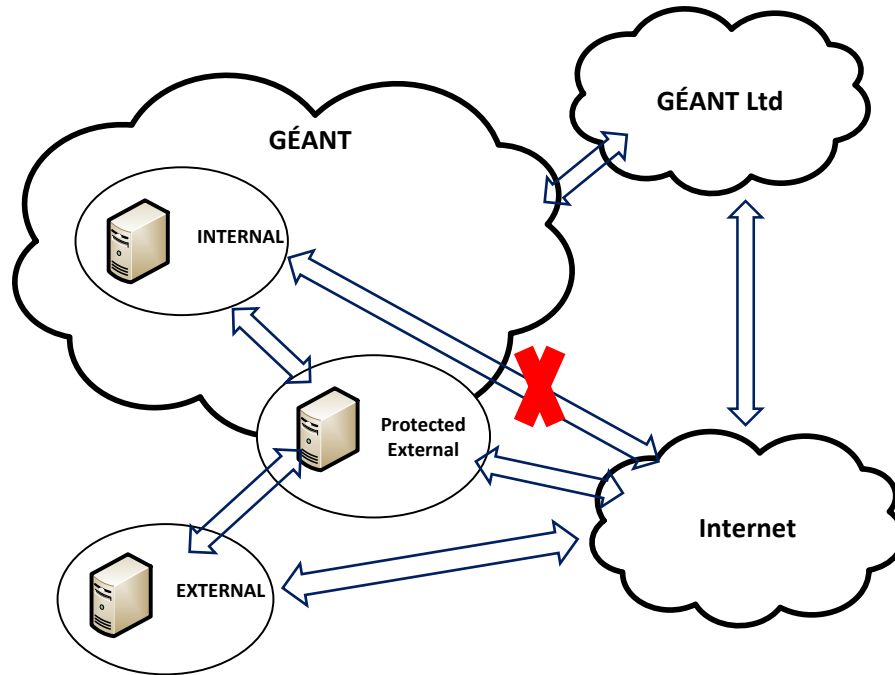
How to Protect Against DDoS?



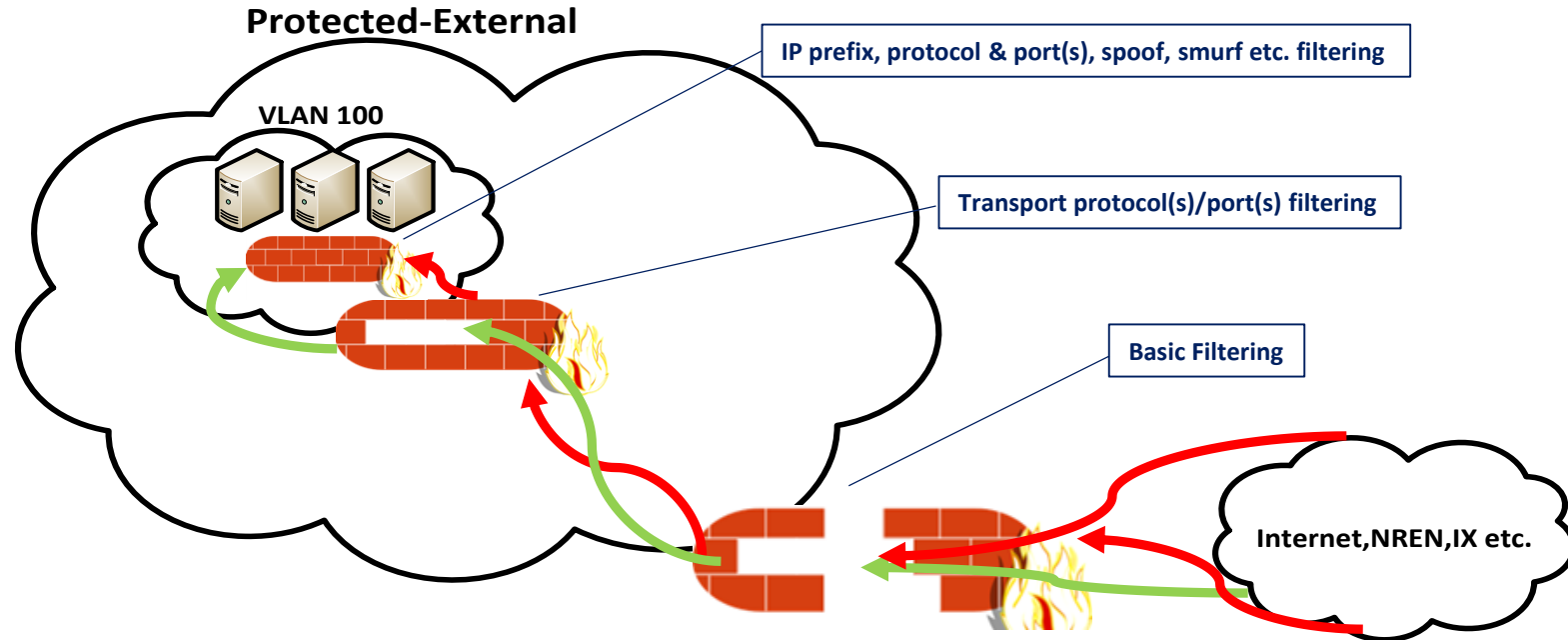




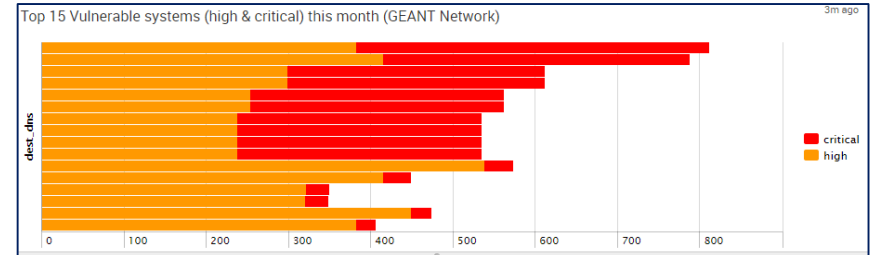
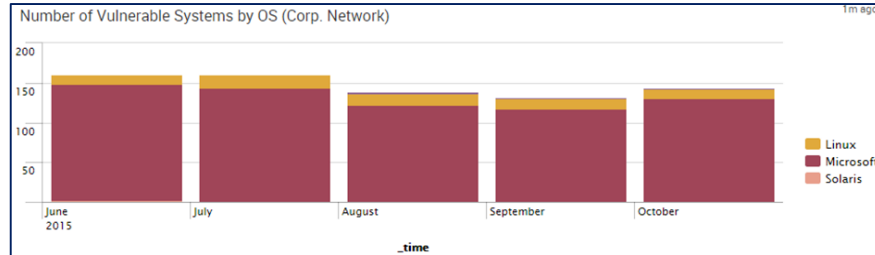
Preventative Controls - Zones



Preventative Controls – Deep Defence



Preventative Controls – Patch Scanning and Management



Number of Vulnerable System by OS

- Asset management
- Areas of attention
- Monthly scans

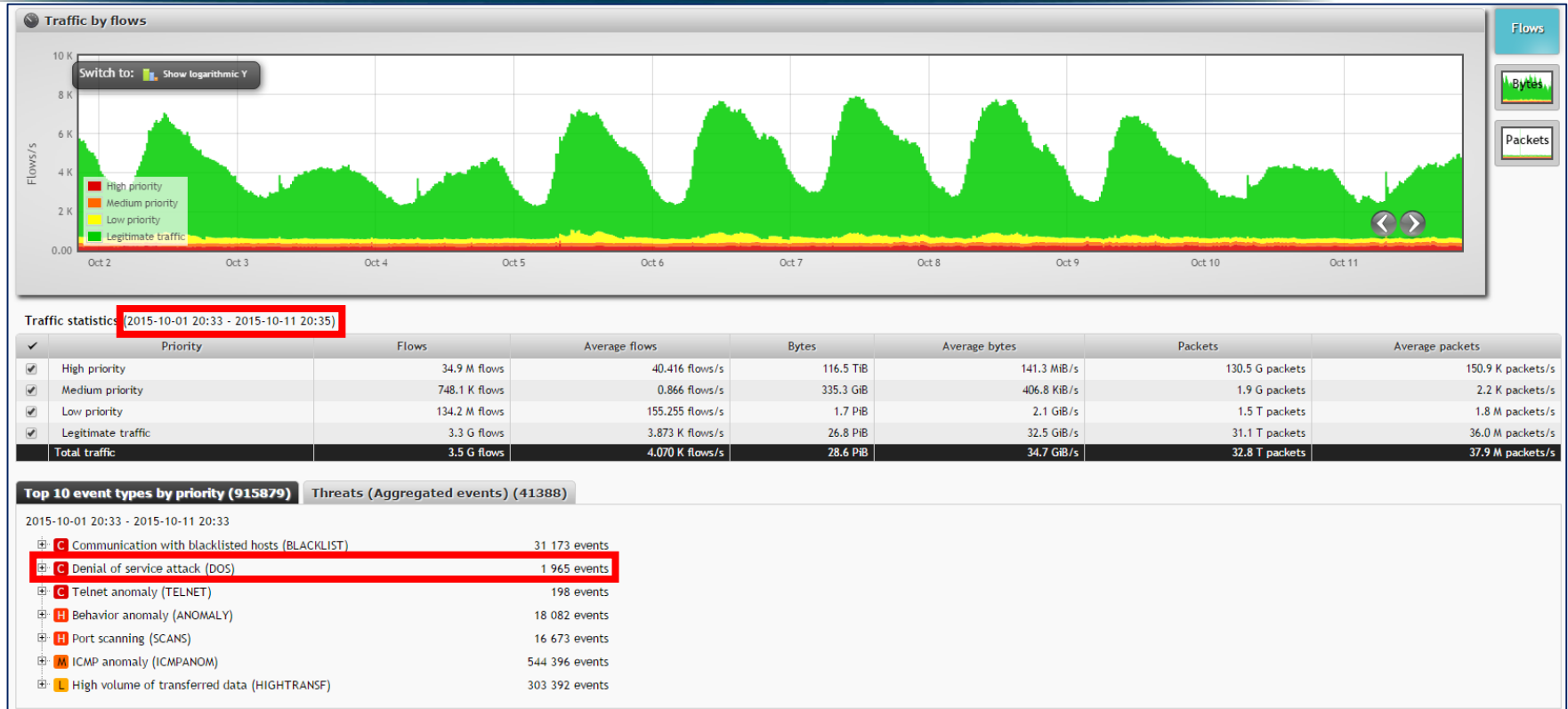
Top 15 Vulnerable Systems for the current month

- By criticality
- Prioritize and remediate weakest ones first
- Monthly scans



**KEEP
CALM
AND
WAIT FOR DDOS**

Detective Controls – NetFlow Monitoring



Detective Controls – NetFlow E-mail Alerts

```

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: [REDACTED].110.30
#Target IPs: [REDACTED].52.61
#Ports: 56118

#Evidence:
Source IP;Source port;Destination IP;Destination
port;Protocol;Timestamp;Duration;Transferred;Packets;Flags;Source AS;Destination AS
[REDACTED].7.110.30;80;[REDACTED].52.61;56118;TCP;2015-10-30
00:22:11.419;0;2840000;2000;.A....:[REDACTED]:[REDACTED]

=====






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,

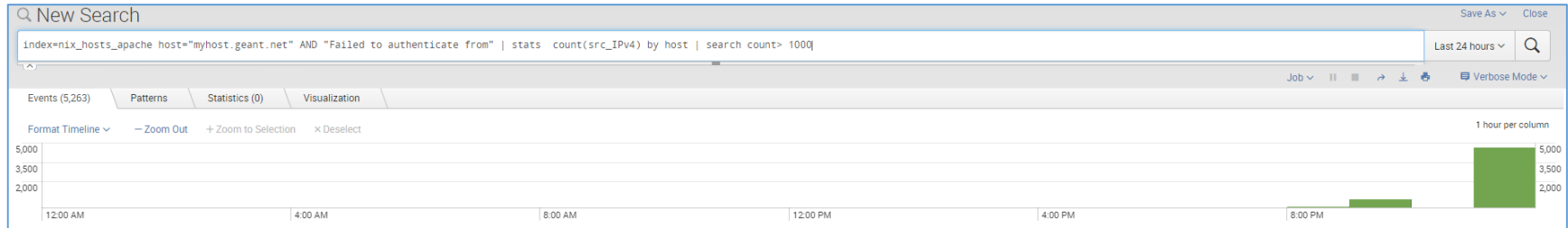
GEANT CERT
cert@oc.geant.net (PGP Key ID: 99833085 / Fingerprint: 3CBF F211 8305 635D 5839 BB27 BA6B
F34A 9983 3085)
Phone no.: +44 (0)1223 866 140
  
```



CRITICAL 	HIGH 	MEDIUM 	LOW 	INFORMATION 
ANOMALY		HTTPDICT		
DOS				
RDPDICT				
SSHDICT				
TELNET				

Detective Controls – Login Rate Monitorin + Iptables + ...

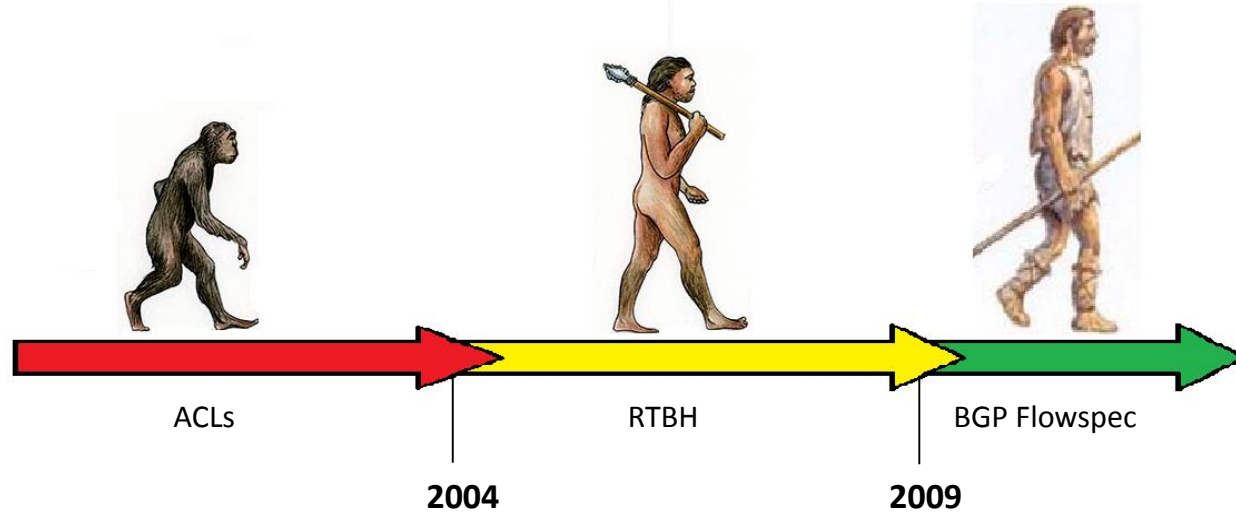
1. `index=nix_hosts_apache "Login failed for user*" | stats count(src_IPv4) by host | search count> 1000`



2. `iptables -I INPUT 5 -m limit --limit 10000/min -j LOG --log-prefix "Possible DDoS: " --log-level 7`
3. Nagios plugins?



Mitigation Controls – ACLs + RTBH + BGP Flowspec



- Doesn't scale
- Time consuming
- Granular
- Less coarse
- Service filtering

- Scalable
- Fast implementation
- No granularity
- Too coarse
- Wide support

- Scalable
- Fast implementation
- Granular
- Less coarse
- No support from older OSs

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


```

[redacted]@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

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

[redacted]@mx1.vie.at.re0> show firewall filter RTBH-count

Filter: RTBH-count
Counters:
Name          Bytes          Packets
RTBH-count    2246512664360  2669500087

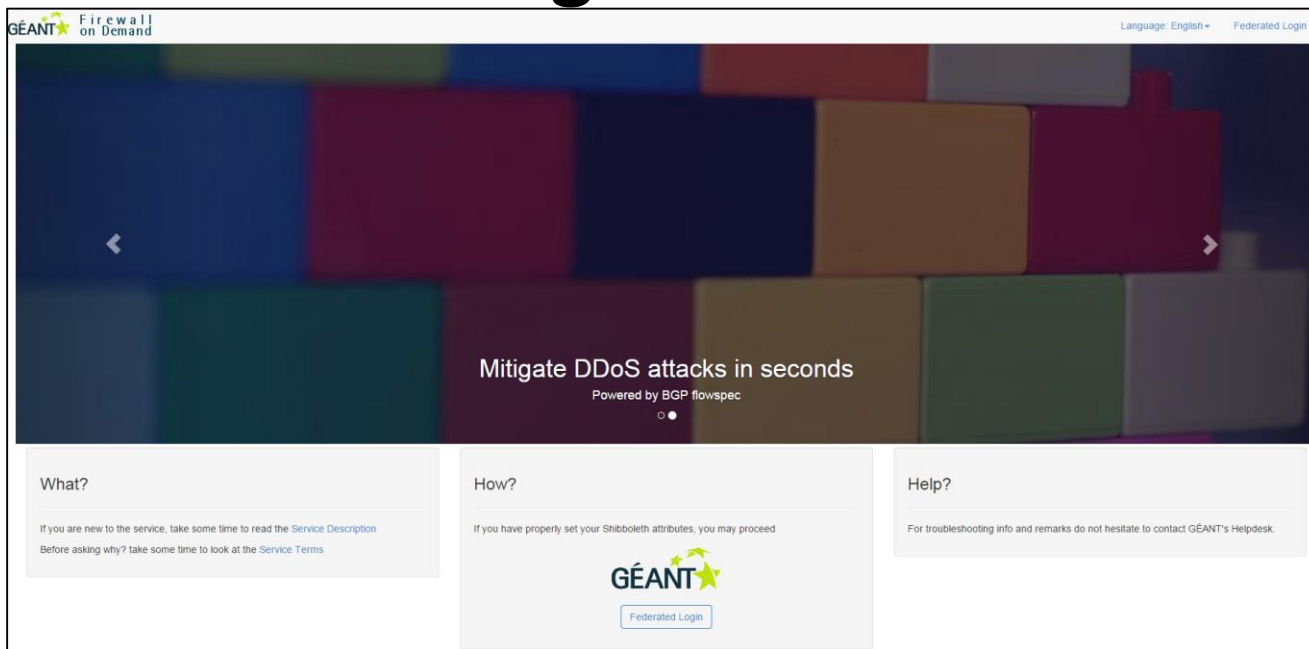
```

Statistics

- 6 RTBH-ed destinations
- 2+ billions of packets blocked

Counters reset every month

fod.geant.net




The screenshot shows the homepage of the GÉANT Firewall on Demand (FoD) service. The header includes the GÉANT logo and 'Firewall on Demand' text on the left, and 'Language: English' and 'Federated Login' on the right. The main banner features a dark background with a colorful, abstract pattern of squares and the text 'Mitigate DDoS attacks in seconds' and 'Powered by BGP flowspec'. Below the banner are three columns: 'What?' with links to 'Service Description' and 'Service Terms', 'How?' with a note about Shibboleth attributes and a 'Federated Login' button, and 'Help?' with a link to the Helpdesk.


Developed and designed by



Firewall Rule

Name

Source Address 

Destination Address 

Protocol(s)

Fragment Type

Select source/destination port(s), or select common port(s) for both source/destination. Hold down "Control", or "Command" on a Mac, to select more than one.

Src. Port(s) **Dest. Port(s)** **Port(s)**

Then Actions

Expires

Comments

FoD WEB GUI

- Dashboard
- Rules
- Add Rule
- Overview
- Admin
- My profile

My rules

Firewall Rules

20 records per page

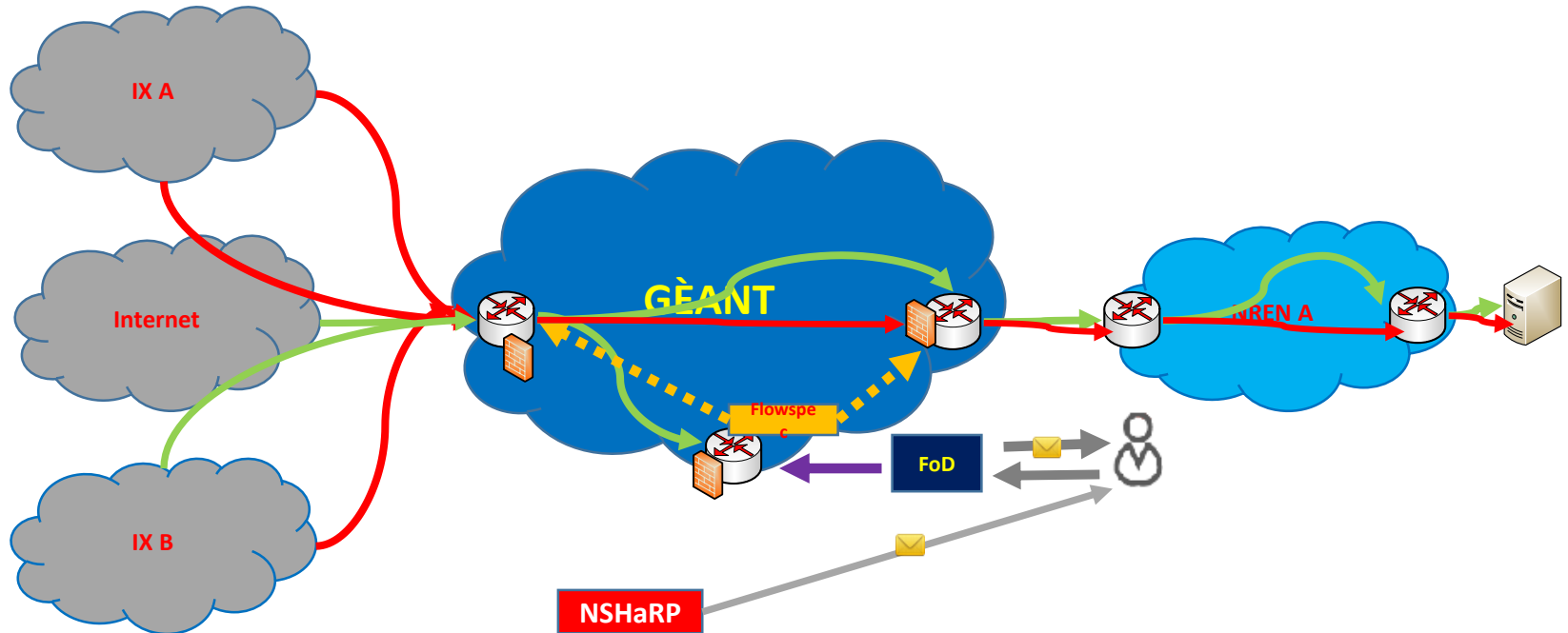
ACTIVE
PENDING
ERROR
DEACTIVATED
Search:

Showing 1 to 4 of 4 entries

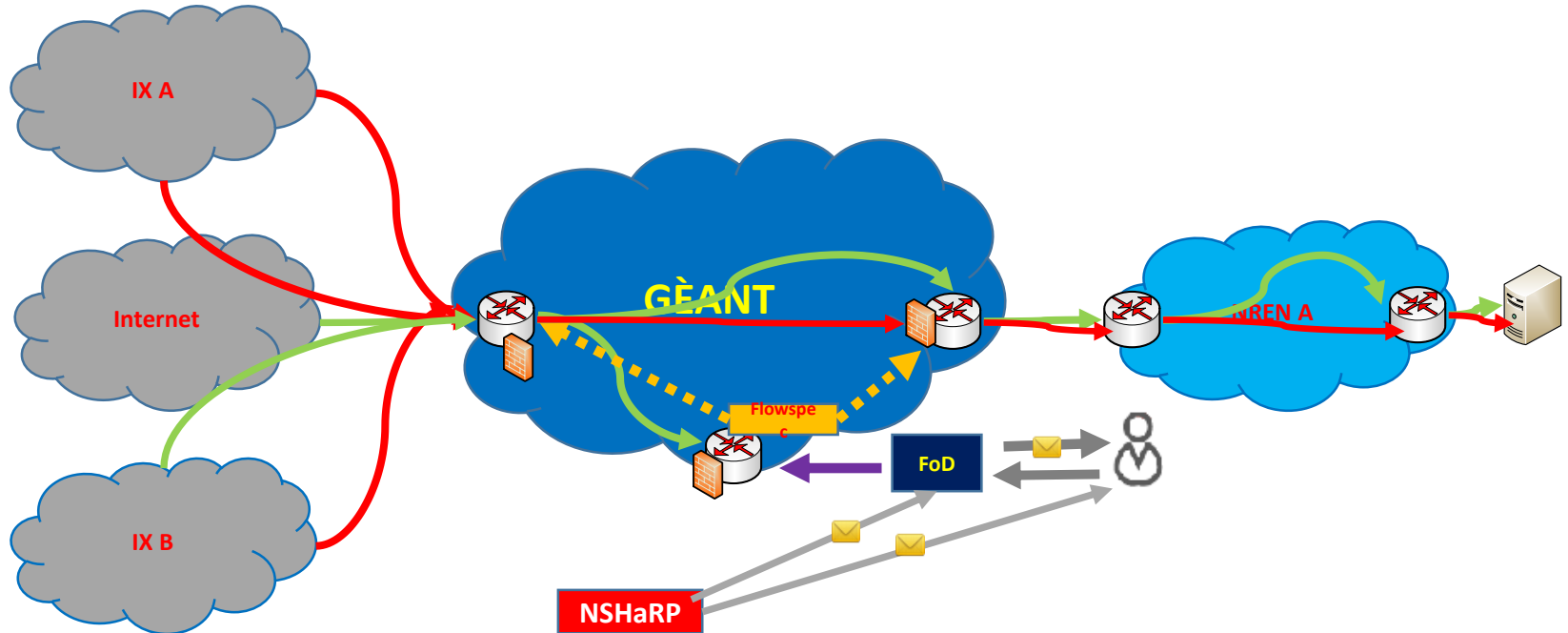
Previous
1
Next

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	Edit Deactivate
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	Edit Deactivate
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	Edit Deactivate

FoD – How Does it Work?



FoD – How Do we Envision it to Work





What do YOU think?

What do YOU think?







Thank you

GEANT Information & Infrastructure Security Team

Evangelos.Spatharas@geant.org



Networks · Services · People
www.geant.org