

# Firewall-on-Demand

GRNET's approach to advanced network security services'  
management via bgp flow-spec and NETCONF

Leonidas Pouloupoulos

<sup>1</sup> [leopoul@noc.grnet.gr](mailto:leopoul@noc.grnet.gr)

<sup>1</sup>NOC/Greek Research and Technology Network

SEE 2/RIPE NCC Regional Meeting - April 2013

# Contents

Introduction

Background

GRNET FoD Implementation

User Interface

Implementation

Future & Synergies

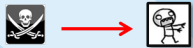
Conclusions

# DDoS illustrated



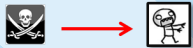
# DDoS illustrated

Attackers use zombies



# DDoS illustrated

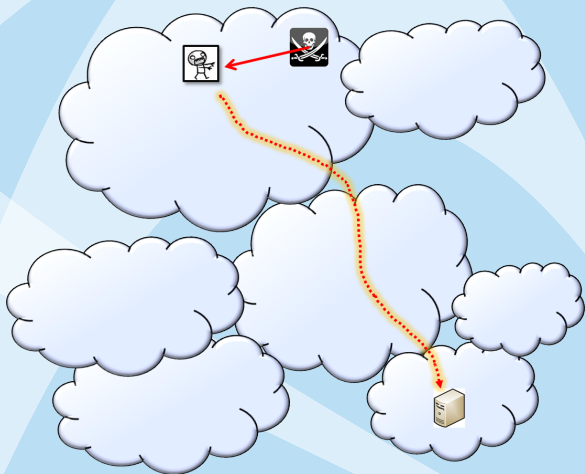
Attackers use zombies



1 zombie:

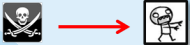


Relative easy to handle



# DDoS illustrated

Attackers use zombies



1 zombie:

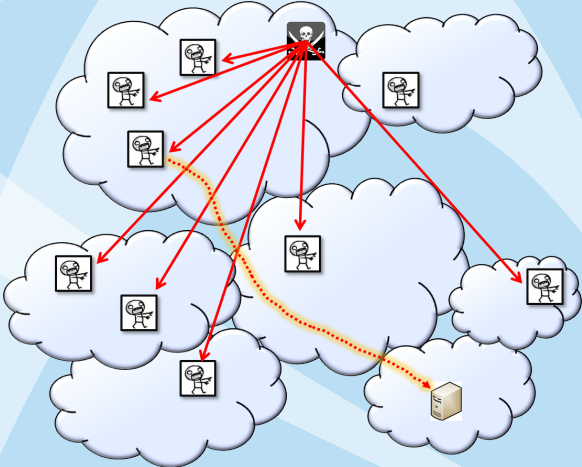


Relative easy to handle

army of zombies

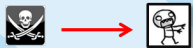


*big problem*



# DDoS illustrated

Attackers use zombies



1 zombie:

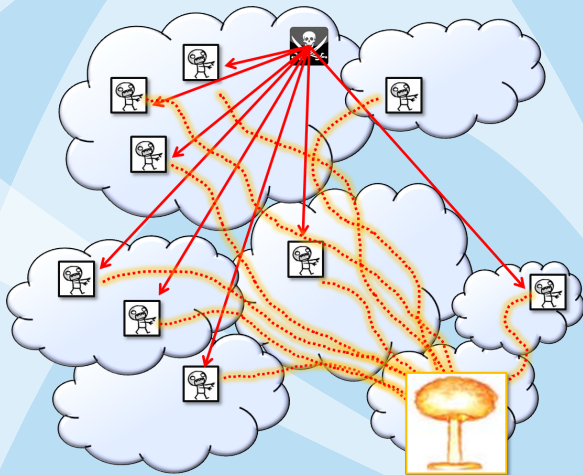


Relative easy to handle

army of zombies



*big problem*



# Motivation

- ▶ Better tools to mitigate *transient* attacks and anomalies (eg DDoS, spambots, viruses, scans, ...),
- ▶ “Better” in terms of
  - ▶ **Granularity:** Per-flow level (Source/Dest IP/Ports, protocol type, DSCP, TCP flag, fragment encoding, ...),
  - ▶ **Action:** Drop, rate-limit, redirect,
  - ▶ **Speed:** quicker (seconds/minutes rather than hours/days)
  - ▶ **Efficiency:** closer to the source, multidomain
  - ▶ **Automation:** integration (eg IDS/IPS, log analyzers,...)
  - ▶ **Manageability:** UI, web, AAI



## **RFC 5575, August 2009: “Dissemination of flow specification rules with BGP”**

Allows BGP to propagate an n-tuple filter with flow matching criteria and actions

- ▶ matching criteria: a combination of source/dest prefix, source/dest port, ICMP type/code, packet size, DSCP, TCP flag, fragment encoding, etc ... , E.g.:
  - ▶ all packets to 10.0.0.1/24 and TCP port 25
  - ▶ all packets to 10.0.0.1/24 from 192.0.0.0/8 and destination port (range [137, 139] or 8080),
- ▶ Filtering actions: accept, discard, rate-limit, sample, redirect, etc ...
- ▶ Information independent of unicast routing (different NLRI), but it is automatically validated against unicast routing.

# Advantages of signaling via BGP

- ▶ Incremental addition to deployed mechanisms,
- ▶ Complexity/scalability issues already solved, flexibility of BGP in adding new services (Multicast, IPv6, L3 VPN, L2 VPN, VPLS),
- ▶ Reuse of:
  - ▶ internal route distribution infrastructure (e.g.: route reflector or confederation design)
  - ▶ existing external relationships (e.g.: inter-domain BGP sessions to a customer network)
- ▶ Trust model in place
  - ▶ normally follows (the well-established trust of) unicast routing
  - ▶ Accept filter when advertised by next-hop for the destination prefix (compare destination address of traffic filtering rule with best match unicast route for this prefix)
    - ▶ Originator of filter and unicast route must be same
    - ▶ No more specifics from a different AS.
- ▶ Can be overridden

# Comparing BGP flowspec with

## **Traditional Firewalls, ACLs**

(Complementary technologies, rather than competitive)

- ▶ No expensive, dedicated hardware
- ▶ Distributed applied as soon as traffic enters the network
- ▶ Actions closer to source
- ▶ Fine-grained
- ▶ Multidomain —easy propagation towards the upstream
- ▶ Easy automation & integration

## **BGP blackhole routing**

- ▶ Flowspec → enhancement of BGP blackhole routing:
- ▶ Less coarse
- ▶ More actions
- ▶ Separate NLRI

# BGP FlowSpec Status

## Vendor support:

- ▶ Juniper: Supported in JUNOS since 7.3 !!!!
- ▶ Cisco: Not supported, no official plan ... But participates in the RFC
- ▶ Other big vendors: No
- ▶ But: Supported by Quagga, ExaBGP and some other routing daemons,
- ▶ IPv6 support: No

# Design Principles (1)

*Goal: A service that will allow GRNET customers to mitigate transient attacks & anomalies at their upstream (GRNET) level. NOT a permanent firewalling service. Rules should be removed at the end of the attack (otherwise auto-expire).*

- ▶ Target audience: GRNET customers (NOCs)
- ▶ Target network: GRNET
- ▶ Web-based tool, shibboleth authentication of the users
- ▶ Customers control internal access via appropriate “Entitlement”

## Design Principles (2)

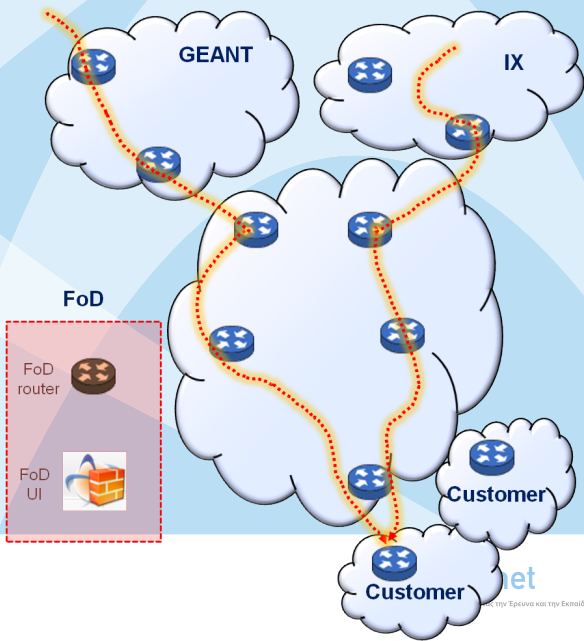
### Functionality:

- ▶ Transient firewall filters across all GRNET routers,
- ▶ Empowered by BGP flowspec
- ▶ Flow granularity:
  - ▶ Source/Destination IPs
  - ▶ Source/Destination ports
  - ▶ More to be added in later versions (eg TCP flags)
- ▶ Flow Manipulation:
  - ▶ Drop
  - ▶ Rate limit to: 10Mbps, 1Mbps, 100Kbps (we can add as many as we want),
  - ▶ More actions in later versions, eg redirect
- ▶ Authorization & Security
  - ▶ Customers → affect traffic destined to themselves
  - ▶ Core network → immune to the tool (in case of bug, misbehavior, compromise)

## Design Principles (3)

- ▶ Programmatic API
  - ▶ REST API to be added in future versions, in order to allow integration with other tools
- ▶ Coding:
  - ▶ Secure
  - ▶ Based on modern technologies,
  - ▶ Open: Open-source license, well-documented, no GRNET-specifics or hardwired stuff
- ▶ Synergies:
  - ▶ Customers
  - ▶ GEANT & NRENs
  - ▶ GRNET or 3rd party security tools. CERT/CIRTs, IPS/IDS, ...

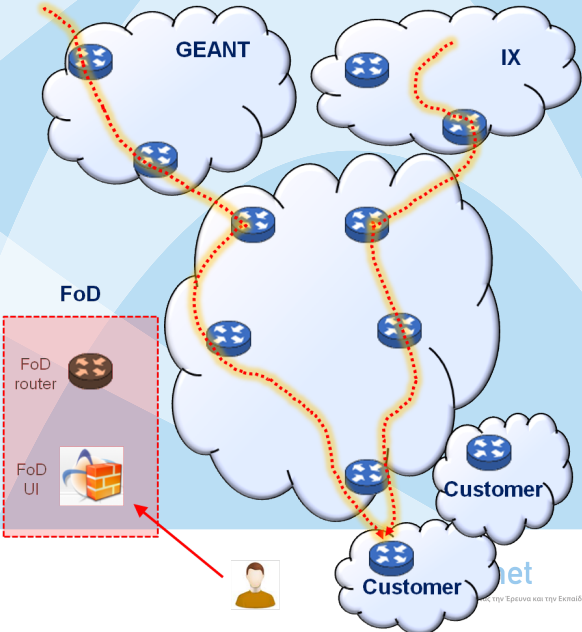
# FoD Operation Overview





# FoD Operation Overview

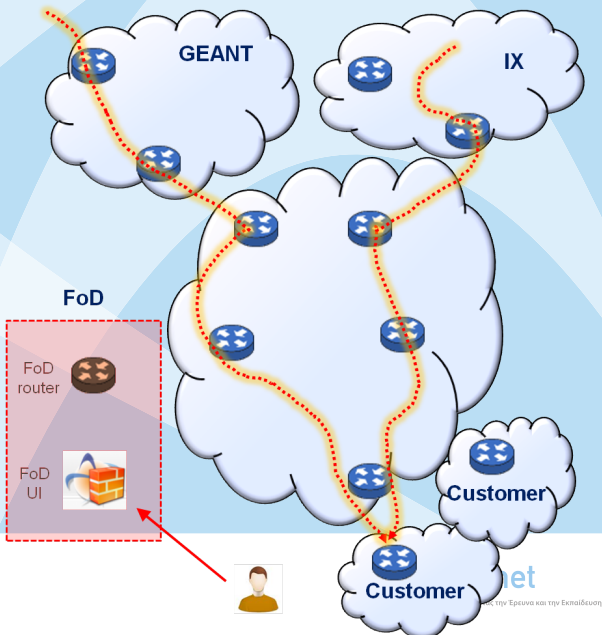
User logs in a web tool and describes flows and actions



# FoD Operation Overview

User logs in a web tool and describes flows and actions

Destination validated against user's IP space

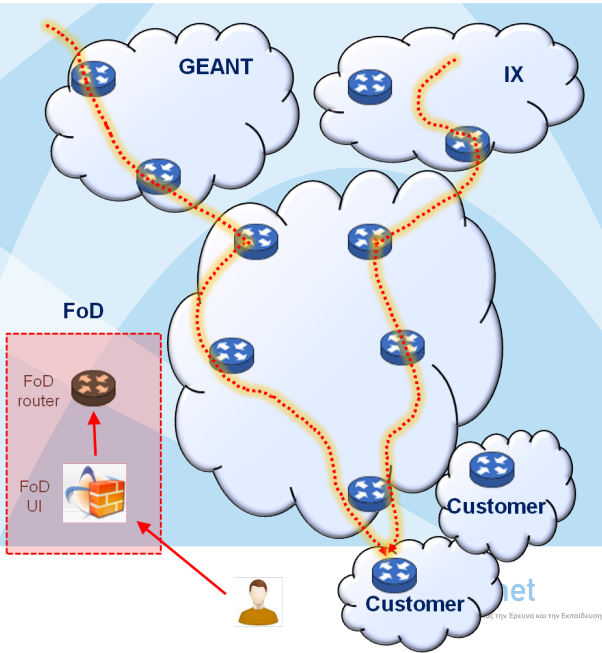


# FoD Operation Overview

User logs in a web tool and describes flows and actions

Destination validated against user's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec



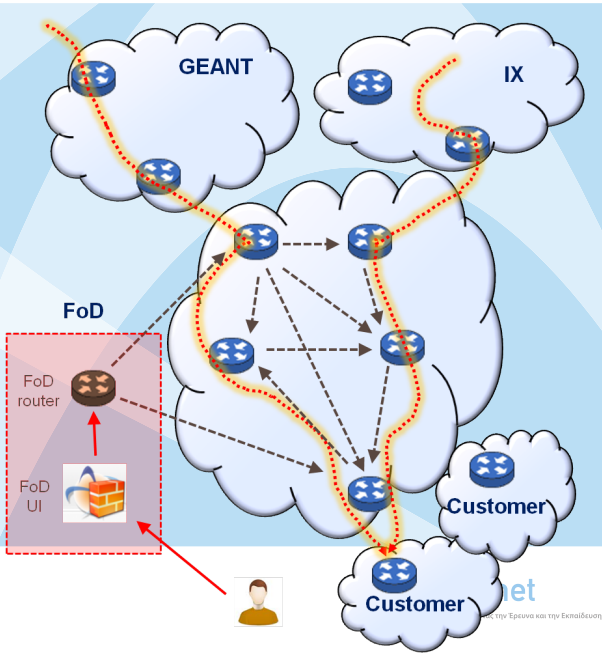
# FoD Operation Overview

User logs in a web tool and describes flows and actions

Destination validated against user's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s). iBGP further propagates the tuples to all GRNET routers.



# FoD Operation Overview

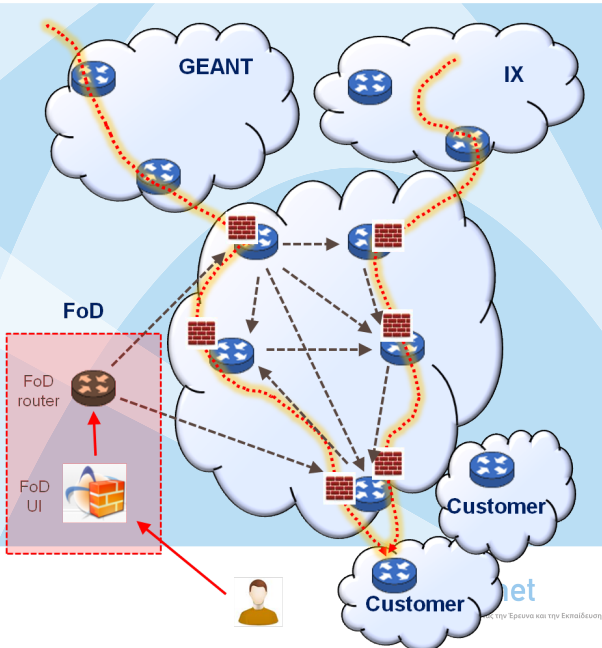
User logs in a web tool and describes flows and actions

Destination validated against user's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s). iBGP further propagates the tuples to all GRNET routers.

Dynamic firewall filters are implemented on all routers



# FoD Operation Overview

User logs in a web tool and describes flows and actions

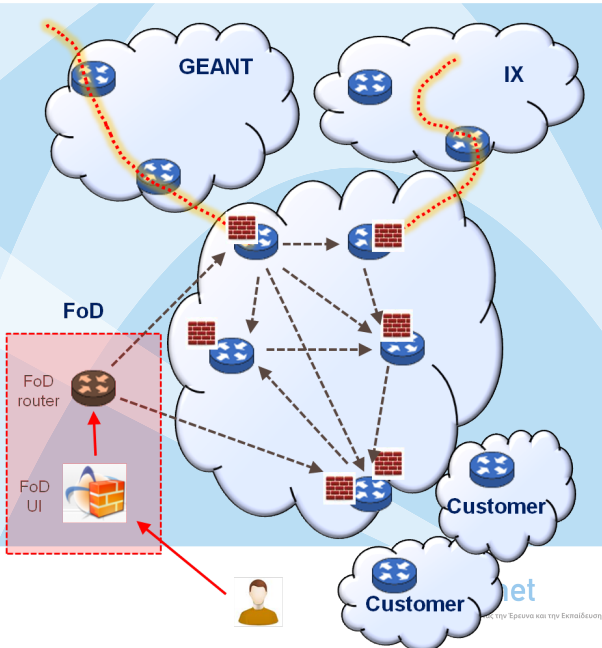
Destination validated against user's IP space

A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s). iBGP further propagates the tuples to all GRNET routers.

Dynamic firewall filters are implemented on all routers

*Attack is mitigated (dropped, rated-limited) upon entrance*



# FoD Operation Overview

User logs in a web tool and describes flows and actions

Destination validated against user's IP space

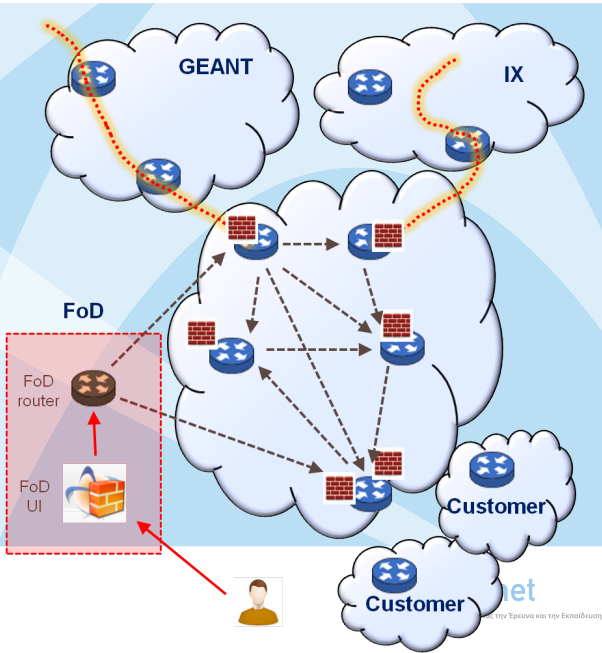
A dedicated router is configured (netconf) to advertise the route via BGP flowspec

eBGP sessions propagate the n-tuple to GRNET router(s).  
iBGP further propagates the tuples to all GRNET routers.

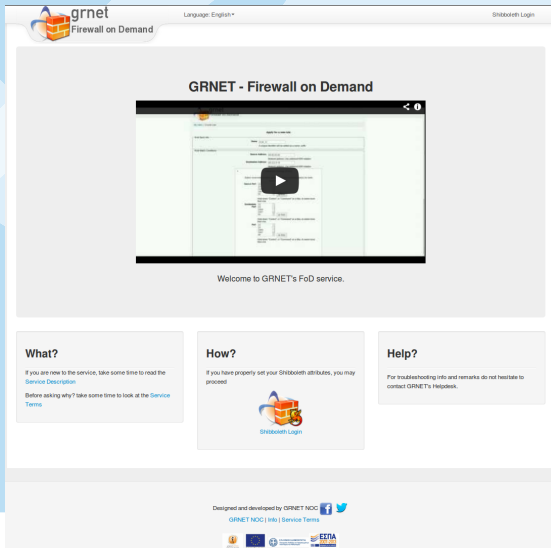
Dynamic firewall filters are implemented on all routers

Attack is mitigated (dropped, rated-limited) upon entrance

*End of attack: Removal via the tool, or auto-expire*



# User Interface #1



The screenshot shows the GRNET Firewall on Demand (FoD) user interface. At the top left is the GRNET logo and the text "grnet Firewall on Demand". To the right, it says "Language: English" and "Shibboleth Login". The main content area features a video player with the title "GRNET - Firewall on Demand" and a play button. Below the video, it says "Welcome to GRNET's FoD service." Below this 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.  
Below this text is the Shibboleth Login logo.
- Help?**  
For troubleshooting info and remarks do not hesitate to contact GRNET's Helpdesk.

At the bottom, it says "Designed and developed by GRNET NOC" with social media icons for Facebook and Twitter. Below that are logos for "GRNET NOC | Info | Service Terms" and various institutional logos including the European Union flag and the Greek Ministry of Education and Religious Affairs (ΕΠΙΤΡΟΧΗ ΕΡΕΥΝΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ).



# User Interface #2

grnet  
Firewall on Demand

My profile Overview Admin Language: English ▼ leopoul@ Logout

My rules


Console Add Rule

Active Suspended Error Pending

Display 25 rules Search:

Name	Match	Then	Status	Applier	Expires	Response	Actions
<a href="#">IERSD_wfi_AP_TXC5TT</a>	Dst Addr: 194.177.1 Src Addr: 0.0.0.0/0 Protocol: icmp Protocol: tcp Protocol: udp	rate-limit: 100k	SUSPENDED	nmilos	26 Mar 13	Rule expired	Reactivate
<a href="#">dns_amp_cdrogos_JU36SA</a>	Dst Addr: 83.212.5 Src Addr: 0.0.0.0/0 Protocol: udp Src Port: 53	discard	SUSPENDED	karaliot	20 Mar 13	Rule expired	Reactivate
<a href="#">test1_NPMWSV</a>	Dst Addr: 155.207.112 Src Addr: 0.0.0.0/0 Protocol: icmp Protocol: tcp Protocol: udp	discard	SUSPENDED	haria	22 Feb 13	Rule expired	Reactivate

# User Interface #3

**grnet**  
Firewall on Demand

[My profile](#) [Overview](#) [Admin](#) [Language: English \\*](#) [leopoul@gnet-hq.admin.gnet.gr](#) [Logout](#)

---

[My rules](#) / [Create rule](#)

### Apply for a new rule

---

**Rule Basic Info**


**Name**

A unique identifier will be added as a name\_suffix


**Admin Options**

**Applier**

**Rule Match Conditions**

**Source Address**   [Any](#)

Network address. Use address/CIDR notation

**Destination Address**  

Network address. Use address/CIDR notation

**Protocol**   
tcp  
udp

**Ports** [Advanced Settings \(Ports\)](#)

**Rule Actions**

**Then**   
rate-limit:1000k  
rate-limit:100k  
rate-limit:1024k

**Expiration**

**Expires**

**Use/Comments**

# User Interface #4

The screenshot shows the gnet Firewall on Demand web interface. At the top, there is a navigation bar with 'My profile', 'Overview', 'Admin', and 'Language: English'. The user 'leopoul@' is logged in. Below the navigation bar, there is a 'My rules' section with a 'Console' button and an 'Add Rule' button. A 'Display' dropdown is set to '25 rules'. A table of rules is visible, with a 'Console' window overlaid on top. The console window shows a log message: '[2013-03-21 01:01:16]: [karaliot@...] Suspending rule : dns\_amp\_cdrosos\_JU36SA Reason: EXPIRED - Result Successfully committed'. The table below the console window shows the following data:

Name	Direction	Then	Status	Applied	Expires	Response	Actions
mmamalis_YEOXVM	Dst Addr: 213.141.254.0/24 Src Addr: 193.105.1.1	deny and log	SUSPENDED	mmamalis@gnet.gr	21 Jan 13	Rule expired	Reactivate
egv5_LLUAHY	Dst Addr: 193.105.1.1 Src Addr: 213.141.254.0/24	discard	SUSPENDED	costas@gnet.gr	30 Nov 12	Rule expired	Reactivate
egv4_FN5SS3	Dst Addr: 193.105.1.1 Src Addr: 112.100.250.0/24	discard	SUSPENDED	costas@gnet.gr	30 Nov 12	Rule expired	Reactivate
egv2_Z168K4	Dst Addr: 193.105.1.1 Src Addr: 41.137.2.2	discard	SUSPENDED	costas@gnet.gr	30 Nov 12	Rule expired	Reactivate

# User Interface #5

The screenshot displays the grnet Firewall on Demand web interface. At the top, the grnet logo and 'Firewall on Demand' text are visible on the left, and navigation links for 'My profile', 'Overview', 'Admin', and 'Language: English' are in the center. The user 'leopoul@' is logged in, with a 'Logout' link on the right.

The main content area is titled 'My rules' and includes a 'Console' button and an 'Add Rule' button. A 'Display' dropdown is set to '25 rules'. A modal dialog box titled 'Suspend Rule' is open, containing the following text:

**Suspend Rule** [X]

You are about to suspend rule **leopoul\_test\_rule\_2PROLS**

Suspending the rule will automatically remove the configuration from the network and mark this rule as inactive.

Are you sure you want to proceed?

[Suspend] [Cancel]

In the background, a table of rules is visible with columns: Name, Applier, Expires, Response, and Actions. The table contains two rows:

Name	Applier	Expires	Response	Actions
leopoul_test_rule_2PROLS	leopoul@	04 Apr 13	Successfully committed	[Edit] [Suspend]
IERSD_wifi_AP_TXC5TT	nm	26 Mar 13	Rule expired	[Reactivate]

# Demo (iperf simulated attack)

```
3] local port 5081 connected with port 38071
[ ID Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[ 1] 0.0-1.0 sec 11.9 MBytes 99.2 Mbits/sec 0.199 ms 101/ 8539 (1.2%)
[ 2] 1.0-2.0 sec 11.8 MBytes 99.0 Mbits/sec 0.096 ms 123/ 8539 (1.4%)
[ 3] 2.0-3.0 sec 11.8 MBytes 98.7 Mbits/sec 0.126 ms 121/ 8518 (1.4%)
[ 4] 3.0-4.0 sec 11.4 MBytes 96.0 Mbits/sec 0.115 ms 349/ 8514 (4.1%)
[ 5] 4.0-5.0 sec 10.7 MBytes 90.1 Mbits/sec 0.110 ms 843/ 8506 (9.9%)
[ 6] 5.0-6.0 sec 11.0 MBytes 99.2 Mbits/sec 0.106 ms 51/ 8499 (0.6%)
[ 7] 6.0-7.0 sec 11.0 MBytes 99.2 Mbits/sec 0.106 ms 111/ 8546 (1.3%)
[ 8] 7.0-8.0 sec 11.8 MBytes 98.9 Mbits/sec 0.098 ms 137/ 8548 (1.6%)
[ 9] 8.0-9.0 sec 11.2 MBytes 94.3 Mbits/sec 0.097 ms 534/ 8548 (6.2%)
[10] 9.0-10.0 sec 11.8 MBytes 99.1 Mbits/sec 0.095 ms 54/ 8481 (0.64%)
[11] 10.0-11.0 sec 12.0 MBytes 100 Mbits/sec 0.096 ms 6/ 8544 (0.07%)
[12] 11.0-12.0 sec 11.9 MBytes 99.1 Mbits/sec 0.091 ms 7/ 8510 (0.082%)
[13] 12.0-13.0 sec 11.9 MBytes 99.5 Mbits/sec 0.113 ms 90/ 8548 (1.1%)
[14] 13.0-14.0 sec 12.0 MBytes 100 Mbits/sec 0.092 ms 5/ 8538 (0.059%)
[15] 14.0-15.0 sec 11.7 MBytes 97.8 Mbits/sec 0.104 ms 229/ 8547 (2.7%)
[16] 15.0-16.0 sec 11.9 MBytes 100 Mbits/sec 0.089 ms 10/ 8530 (0.12%)
[17] 16.0-17.0 sec 11.3 MBytes 94.4 Mbits/sec 0.153 ms 440/ 8469 (5.2%)
[18] 17.0-18.0 sec 12.1 MBytes 101 Mbits/sec 0.123 ms 6/ 8623 (0%)
[19] 18.0-19.0 sec 11.9 MBytes 100 Mbits/sec 0.105 ms 17/ 8541 (0.2%)
[20] 19.0-20.0 sec 11.4 MBytes 95.3 Mbits/sec 0.126 ms 441/ 8546 (5.2%)
[21] 20.0-21.0 sec 10.6 MBytes 89.0 Mbits/sec 0.048 ms 908/ 8479 (11%)
[22] 21.0-22.0 sec 10.1 MBytes 84.5 Mbits/sec 0.069 ms 1092/ 8436 (13%)
[23] 22.0-23.0 sec 11.8 MBytes 99.2 Mbits/sec 0.099 ms 447/ 8802 (5%)
[24] 23.0-24.0 sec 11.8 MBytes 99.1 Mbits/sec 0.095 ms 116/ 8544 (1.4%)
[25] 24.0-25.0 sec 12.0 MBytes 100 Mbits/sec 0.097 ms 0/ 8545 (0%)
[26] 25.0-26.0 sec 11.7 MBytes 98.0 Mbits/sec 0.101 ms 191/ 8528 (2.2%)
[27] 26.0-27.0 sec 11.4 MBytes 95.5 Mbits/sec 0.130 ms 425/ 8543 (5%)
[28] 27.0-28.0 sec 11.9 MBytes 99.8 Mbits/sec 0.109 ms 58/ 8548 (0.68%)
[29] 28.0-29.0 sec 11.3 MBytes 92.0 Mbits/sec 0.094 ms 660/ 8547 (7.7%)
[30] 29.0-30.0 sec 12.0 MBytes 100 Mbits/sec 0.108 ms 8/ 8546 (0.094%)
[31] 30.0-31.0 sec 12.0 MBytes 100 Mbits/sec 0.108 ms 14/ 8540 (0.16%)
[32] 31.0-32.0 sec 9.8 MBytes 98.5 Mbits/sec 0.121 ms 167/ 8544 (2%)
[33] 32.0-33.0 sec 9.8 MBytes 82.7 Mbits/sec 0.118 ms 10/ 7908 (0.14%)
[34] 33.0-34.0 sec 12.9 KBytes 106 Kbits/sec 0.121 ms 8992/ 9001 (1e+02%)
[35] 34.0-35.0 sec 10.9 KBytes 100 Kbits/sec 0.109 ms 9209/ 9210 (1e+02%)
[36] 35.0-36.0 sec 10.0 KBytes 82.3 Kbits/sec 0.088 ms 7369/ 7376 (1e+02%)
[37] 36.0-37.0 sec 12.9 KBytes 106 Kbits/sec 0.077 ms 9208/ 9217 (1e+02%)
[38] 37.0-38.0 sec 12.9 KBytes 106 Kbits/sec 1.075 ms 9211/ 9220 (1e+02%)
[39] 38.0-39.0 sec 10.0 KBytes 82.3 Kbits/sec 0.725 ms 7369/ 7376 (1e+02%)
[40] 39.0-40.0 sec 12.9 KBytes 106 Kbits/sec 0.068 ms 9173/ 9182 (1e+02%)
[41] 40.0-41.0 sec 12.9 KBytes 106 Kbits/sec 0.297 ms 8921/ 8930 (1e+02%)
[42] 41.0-42.0 sec 10.0 KBytes 82.3 Kbits/sec 0.237 ms 7388/ 7395 (1e+02%)
[43] 42.0-43.0 sec 12.9 KBytes 106 Kbits/sec 0.31 ms 9110/ 9119 (1e+02%)
[44] 43.0-44.0 sec 10.0 KBytes 82.3 Kbits/sec 0.318 ms 7388/ 7312 (1e+02%)
[45] 44.0-45.0 sec 12.9 KBytes 106 Kbits/sec 0.228 ms 9183/ 9184 (1e+02%)
[46] 45.0-46.0 sec 10.0 KBytes 82.3 Kbits/sec 0.178 ms 9042/ 9051 (1e+02%)
[47] 46.0-47.0 sec 11.5 KBytes 94.1 Kbits/sec 0.140 ms 7206/ 7214 (1e+02%)
[48] 47.0-48.0 sec 12.9 KBytes 106 Kbits/sec 0.182 ms 9223/ 9232 (1e+02%)
[49] 48.0-49.0 sec 12.9 KBytes 106 Kbits/sec 0.522 ms 9197/ 9206 (1e+02%)
[50] 49.0-50.0 sec 10.0 KBytes 82.3 Kbits/sec 0.360 ms 7360/ 7367 (1e+02%)
[51] 50.0-51.0 sec 12.9 KBytes 106 Kbits/sec 1.493 ms 9093/ 9102 (1e+02%)
[52] 51.0-52.0 sec 12.9 KBytes 106 Kbits/sec 1.665 ms 9285/ 9294 (1e+02%)
[53] 52.0-53.0 sec 10.0 KBytes 82.3 Kbits/sec 1.108 ms 7189/ 7196 (1e+02%)
[54] 53.0-54.0 sec 12.9 KBytes 106 Kbits/sec 0.658 ms 9148/ 9157 (1e+02%)
[55] 54.0-55.0 sec 10.0 KBytes 82.3 Kbits/sec 0.490 ms 7347/ 7354 (1e+02%)
[56] 55.0-56.0 sec 12.9 KBytes 106 Kbits/sec 6.294 ms 8662/ 8671 (1e+02%)
[57] 56.0-57.0 sec 12.9 KBytes 106 Kbits/sec 3.972 ms 9068/ 9077 (1e+02%)
[58] 57.0-58.0 sec 10.0 KBytes 82.3 Kbits/sec 2.983 ms 6965/ 6972 (1e+02%)
[59] 58.0-59.0 sec 12.9 KBytes 106 Kbits/sec 3.221 ms 8780/ 8789 (1e+02%)
[60] 59.0-60.0 sec 12.9 KBytes 106 Kbits/sec 2.174 ms 8521/ 8530 (1e+02%)
```

A 100Mbps attack

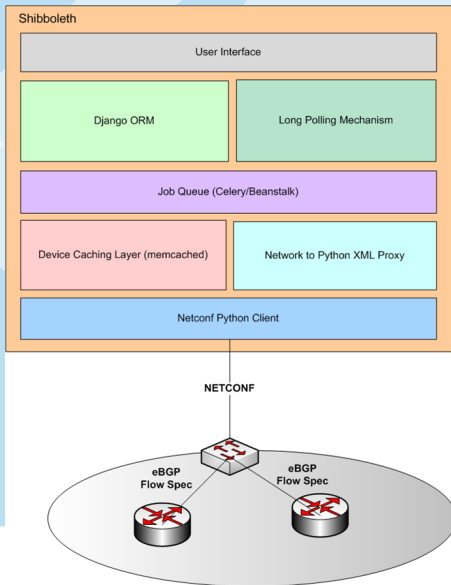
User presses "Apply" in rule creation form

Typically less than 15 seconds

Rule is propagated via eBGP to core router. Attack is mitigated (rate limit)

Flow limited to 100Kbps

# Implementation - Architecture



# Implementation - Technologies

- ▶ Open Source project
  - ▶ Python Django ORM
  - ▶ jQuery Javascript lib, Bootstrap CSS
- ▶ Multicomponent architecture
  - ▶ Shibboleth: User authentication based on special attribute
  - ▶ Django: UI rendering & db modeling
  - ▶ Long polling: fetch updates without reloading
    - ▶ used in: facebook chat, twitter updates
  - ▶ Celery/beanstalk: apply configuration without locks
  - ▶ npxy: Network XML to python classes proxy
    - ▶ Dev & maint by GRNET NOC developer (Leonidas Pouloupoulos)
  - ▶ Ncclient: python netconf client (ncclient)
    - ▶ Maintained by GRNET NOC developer (Leonidas Pouloupoulos)
  - ▶ Caching, cron jobs

# Information Flow

- ▶ User login
  - ▶ Rule management (Creation, removal)
  - ▶ Notifications, status
- 
- ▶ Transform rules to python objects
  - ▶ DB operations
  - ▶ Transform python objects to netconf XML configuration
  - ▶ Apply XML configuration via NETCONF to device
- 
- ▶ Save received configuration to device (switch)
  - ▶ Propagate rule via eBGP to peer routers
  - ▶ Rule filters and acts on matching flows



# Information Flow

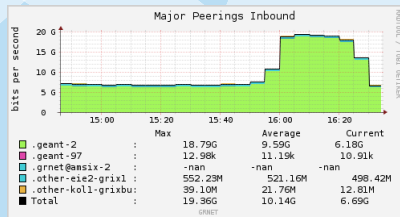
- ▶ User login
  - ▶ Rule management (Creation, removal)
  - ▶ Notifications, status
- 
- ▶ Transform rules to python objects
  - ▶ DB operations
  - ▶ Transform python objects to netconf XML configuration
  - ▶ Apply XML configuration via NETCONF to device
- 
- ▶ Save received configuration to device (switch)
  - ▶ Propagate rule via eBGP to peer routers
  - ▶ Rule filters and acts on matching flows

# Information Flow

- ▶ User login
  - ▶ Rule management (Creation, removal)
  - ▶ Notifications, status
- 
- ▶ Transform rules to python objects
  - ▶ DB operations
  - ▶ Transform python objects to netconf XML configuration
  - ▶ Apply XML configuration via NETCONF to device
- 
- ▶ Save received configuration to device (switch)
  - ▶ Propagate rule via eBGP to peer routers
  - ▶ Rule filters and acts on matching flows

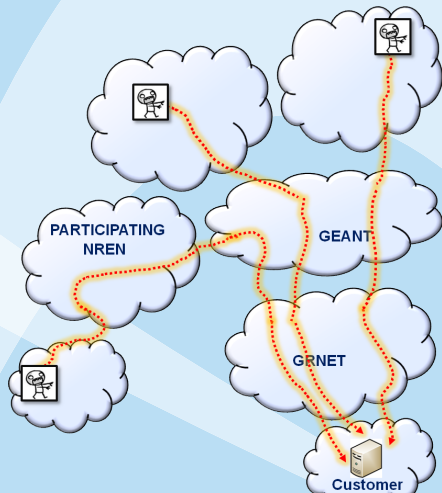
# Status

- ▶ Latest stable
- ▶ Production GRNET network
- ▶ <http://fod.grnet.gr/>
- ▶ Successful mitigation of aprox. 20 attacks in 2 months

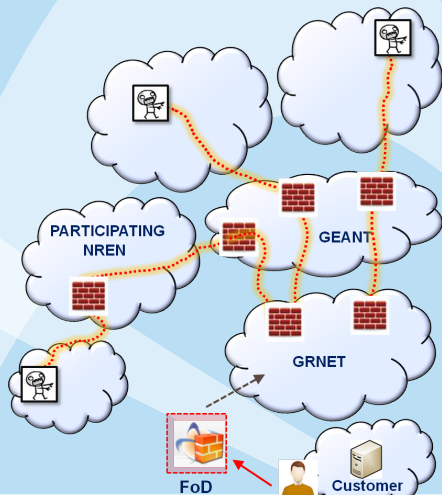


- ▶ Source code:
  - ▶ <http://code.grnet.gr/>

# Expanding the service to the GEANT community



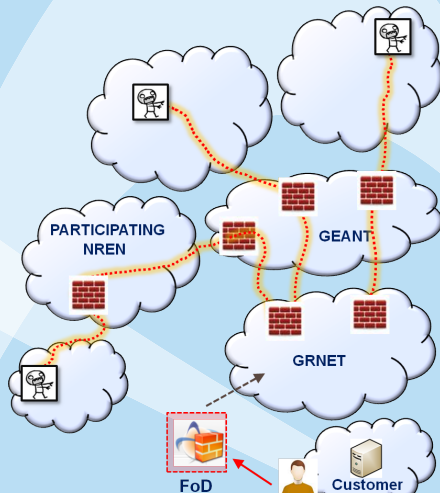
# Expanding the service to the GEANT community



# Expanding the service to the GEANT community

## Phase 1: GEANT participation

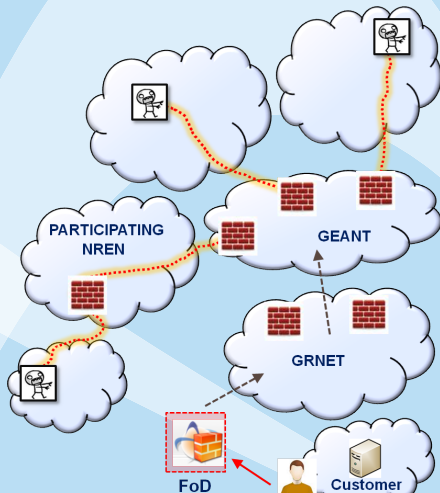
- ▶ Routers accept BGP flowspec NLRI
- ▶ Establish BGP peerings with GRNET (protected by route-maps)



# Expanding the service to the GEANT community

## Phase 1: GEANT participation

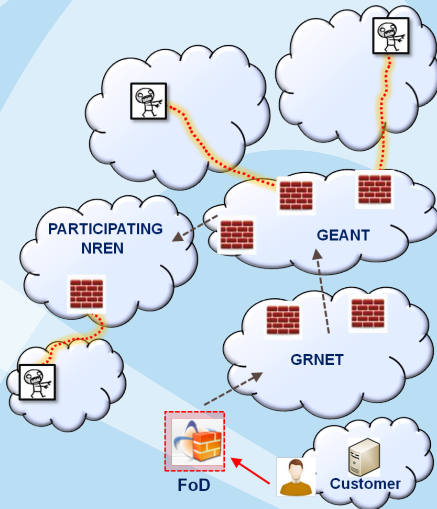
- ▶ Routers accept BGP flowspec NLRI
- ▶ Establish BGP peerings with GRNET (protected by route-maps)
- ▶ GRNET filters are applied at GEANT level



# Expanding the service to the GEANT community

## Phase 1: GEANT participation

- ▶ Routers accept BGP flowspec NLRI
- ▶ Establish BGP peerings with GRNET (protected by route-maps)
- ▶ GRNET filters are applied at GEANT level



## Phase 2: NREN participation

- ▶ NRENs → propagate filters through bgp peerings instead of UI



## Synergies with security team

- ▶ Connect to the domain's IPS/IDS, honeypots, ...
- ▶ Connect to GEANT anomaly detection tool
- ▶ Connect to any CERT/CIRT team that we trust

“Soft” actions can make adoption easier

- ▶ Rate-limit instead of drop

# Service Outreach

*Project is open-source*

Requirements to run the service:

- ▶ Juniper on your network
- ▶ A vm to host the service
- ▶ A juniper router, dedicated to the service
  - ▶ L3 switches are sufficient
  - ▶ A “virtual router” (olive VM) could also be used
- ▶ Shibboleth recommended (but can be omitted)
- ▶ DB: customers → IP space (auth)
  - ▶ whois → DB is implemented

## Still in doubt?


- ▶ Try the existing instance of the service (@GRNET) on **your** network
- ▶ Multihop-BGP peering between our service and your routers
- ▶ BGP filters (on your side) can be used to restrict the effects on a specific “testing” IP range.


Thank you

Questions?

Work carried-out by Leonidas Pouloupoulos, Michalis Mamalis & Andreas Polyraakis

GRNET NOC <http://noc.grnet.gr/>

 Like: <https://facebook.com/noc.grnet.gr/>

 Follow: <https://twitter.com/grnetnoc>