Firewall-on-Demand

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

Leonidas Poulopoulos
[1] leopoul@noc.grnet.gr

[1]NOC/Greek Research and Technology Network

SEE 2/RIPE NCC Regional Meeting - April 2013

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Contents

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

DDoS illustrated

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

DDoS illustrated

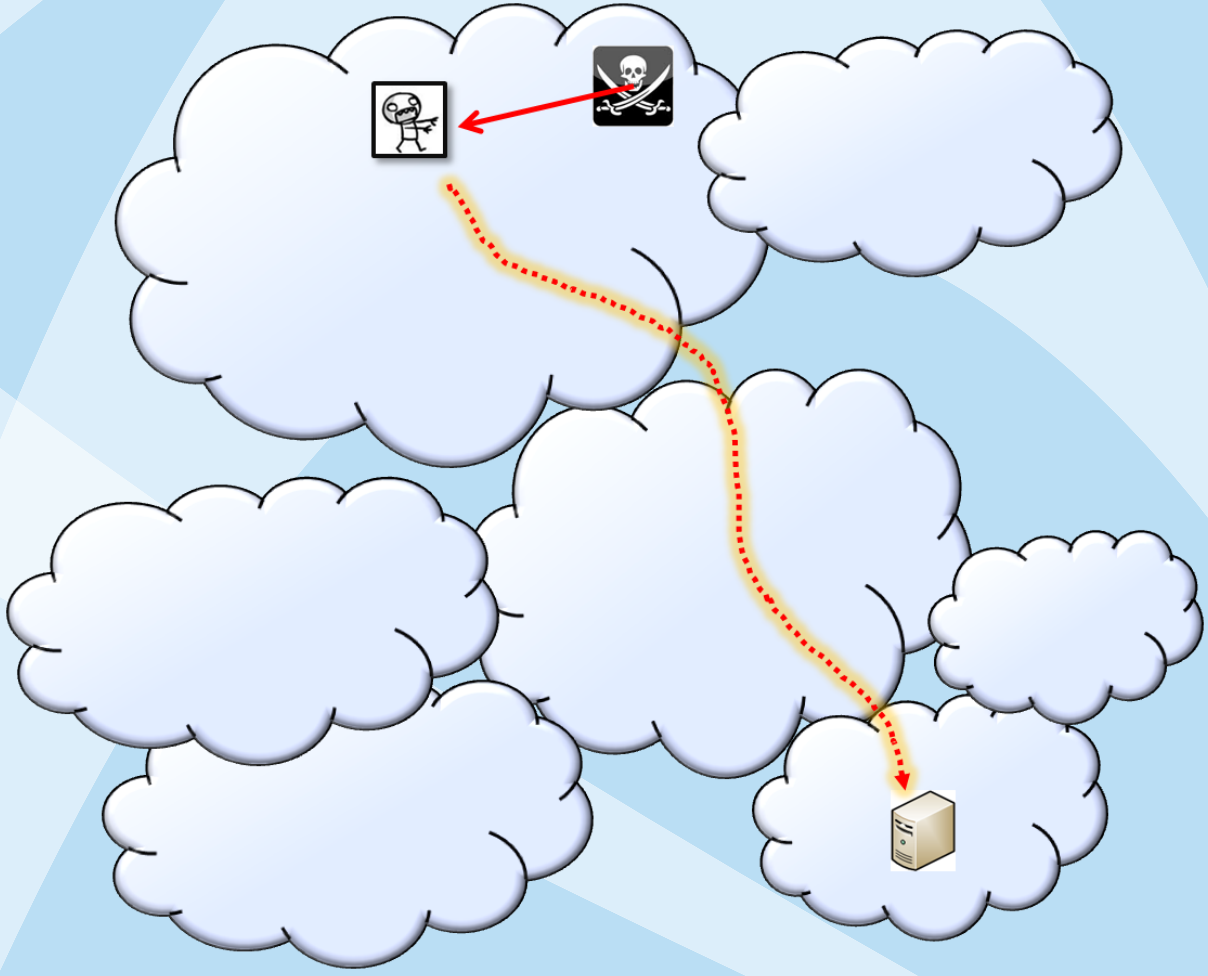
Attackers use zombies

DDoS illustrated

Attackers use zombies

1 zombie:

Relative easy to handle



DDoS illustrated

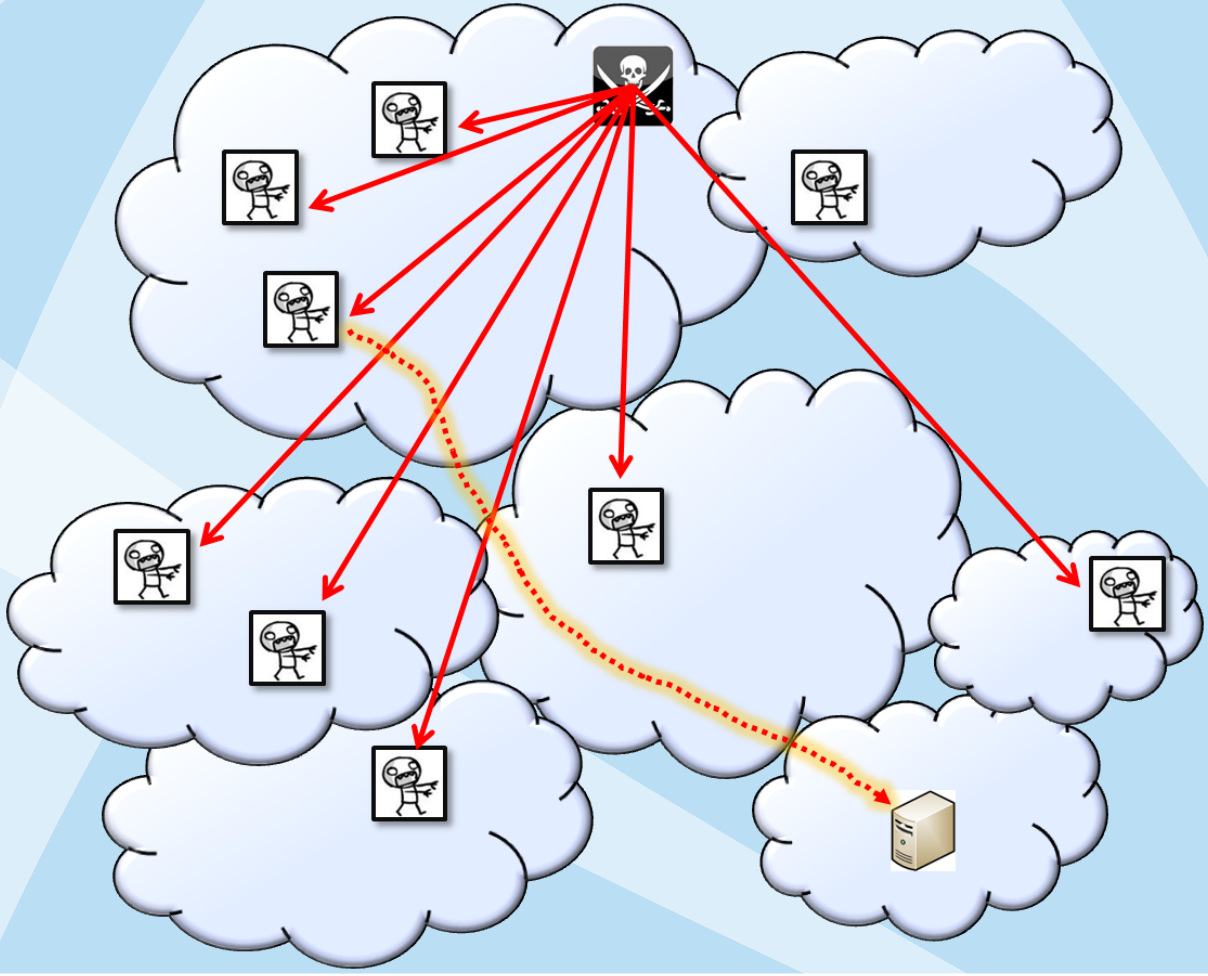
Attackers use zombies

1 zombie:

Relative easy to handle

army of zombies

big problem



DDoS illustrated

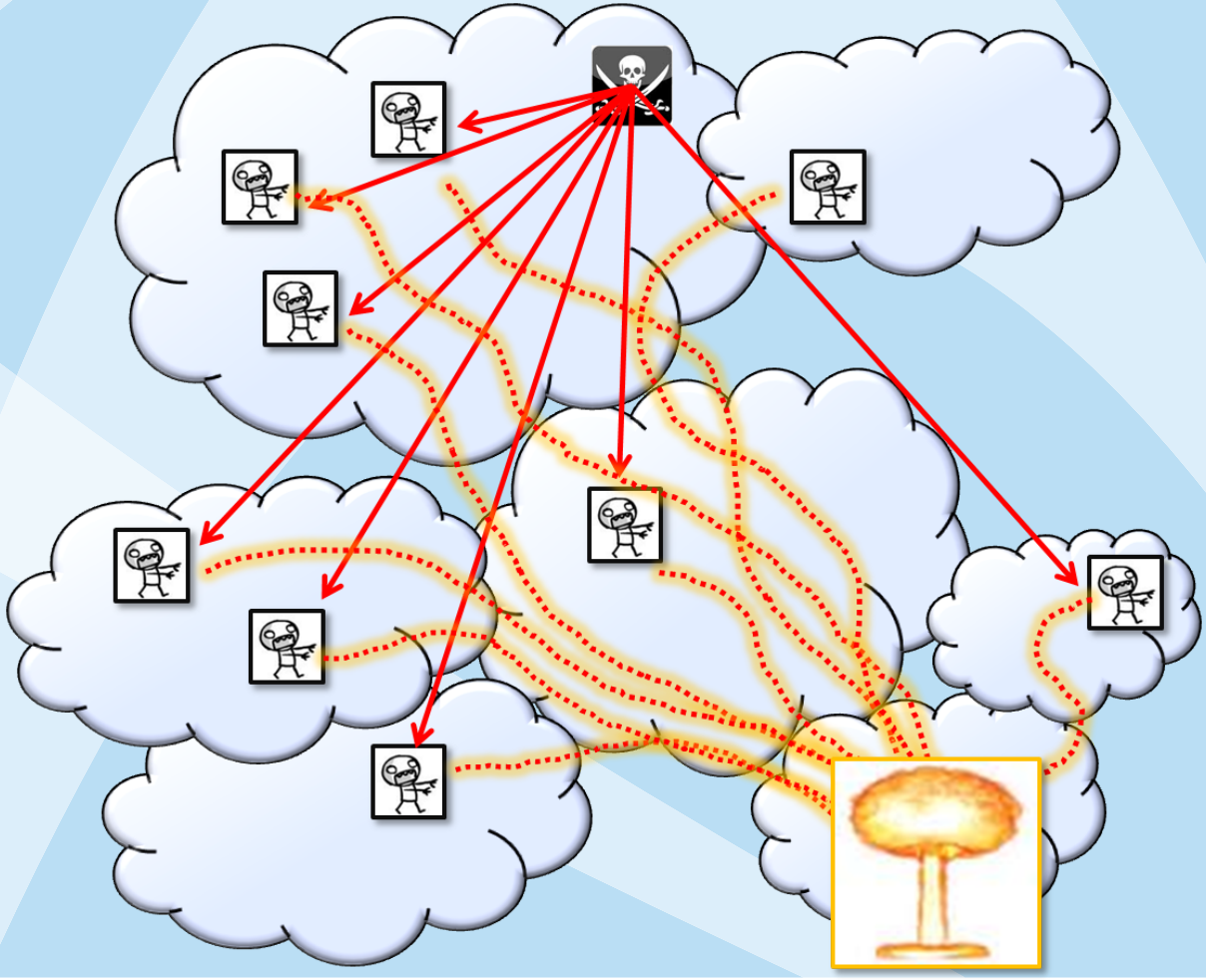
Attackers use zombies

1 zombie:

Relative easy to handle

army of zombies

big problem



grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

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

BGP FlowSpec

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 $\rightarrow$ 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)

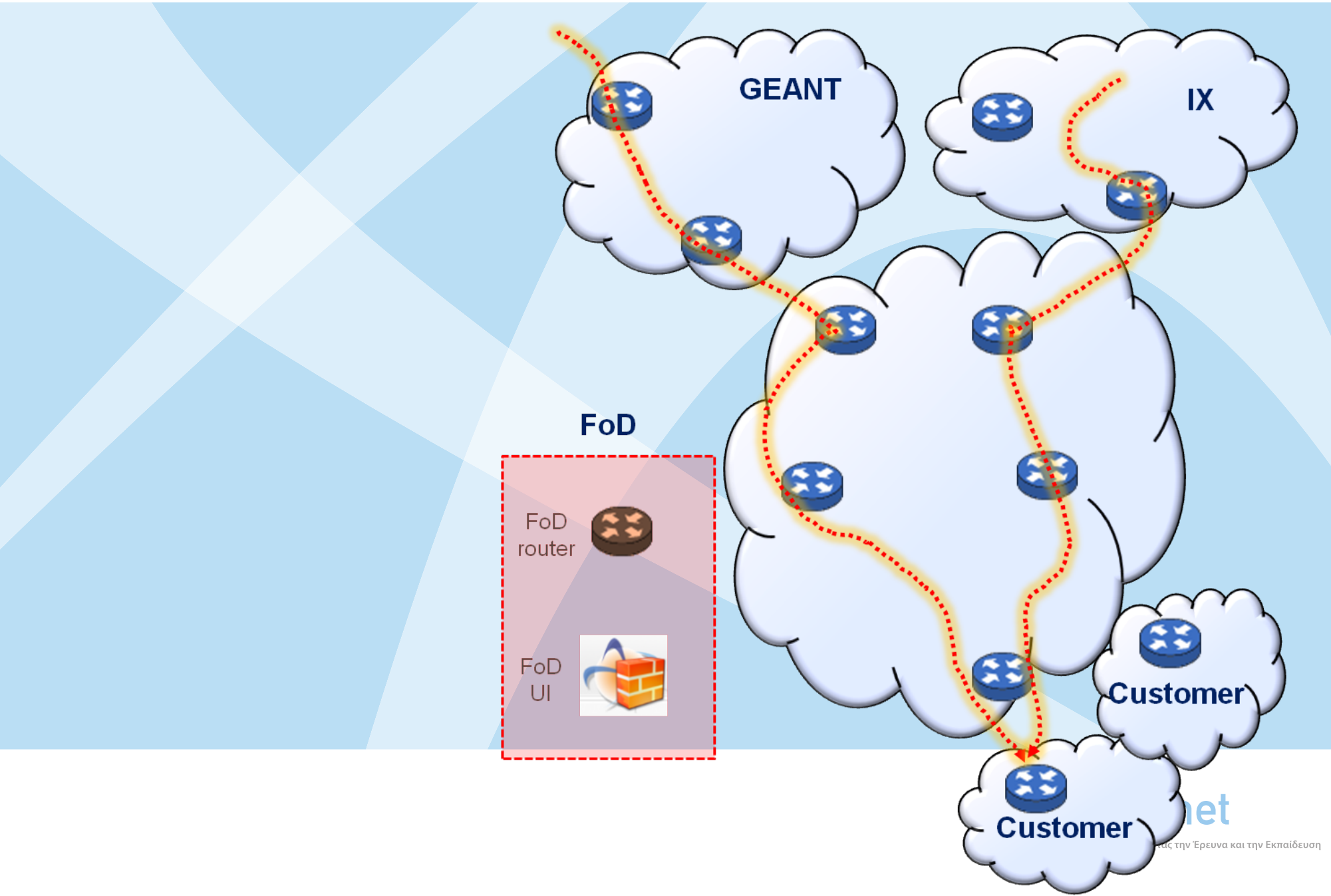
Functionality:

- 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 $\rightarrow$ affect traffic destined to themselves
  - Core network $\rightarrow$ immune to the tool (in case of bug, misbehavior, compromise)

Design Principles (3)

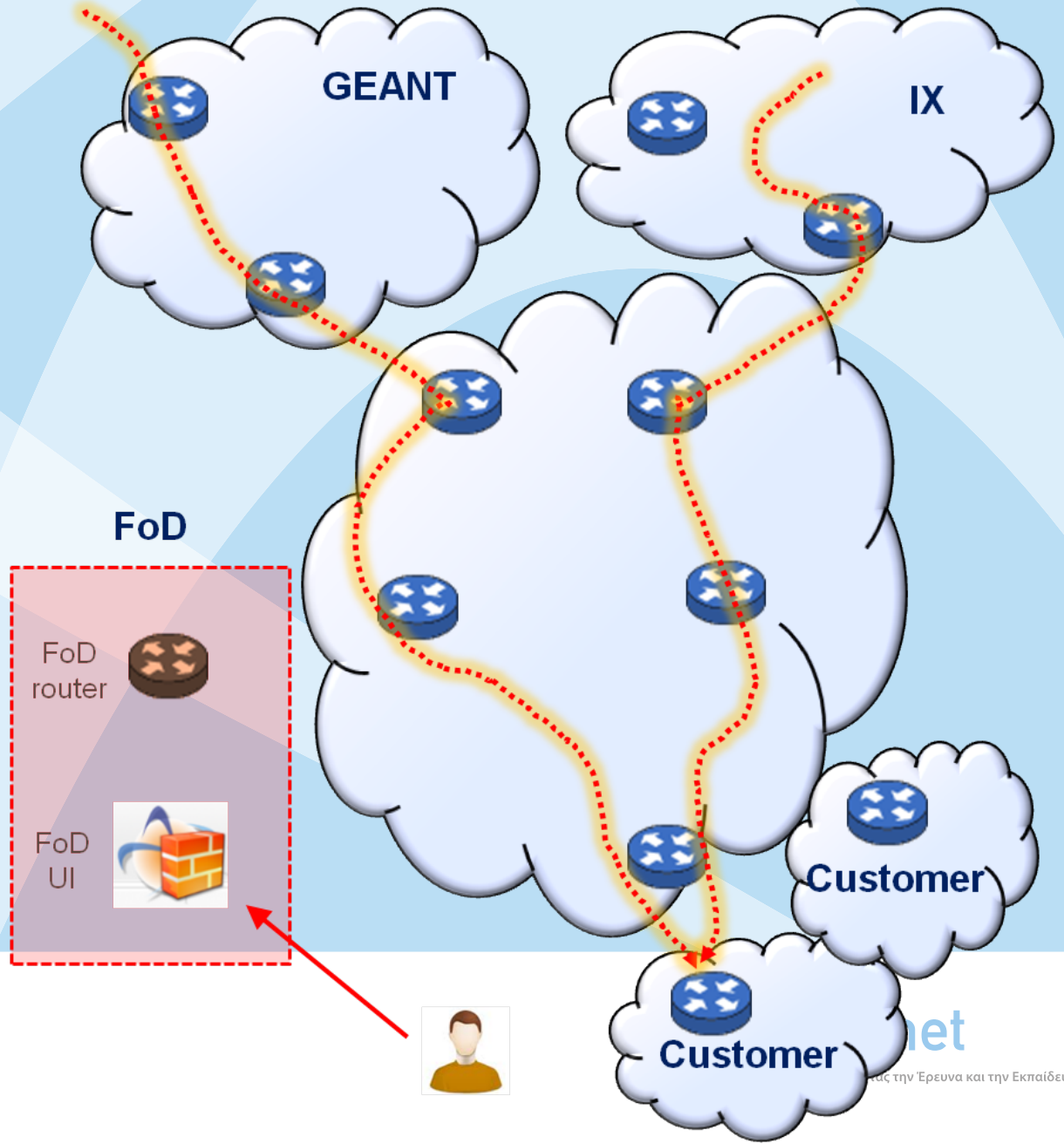
- Programmatic API
  - REST API to be added in future versions, in order to allow integration with other tools
- Coding:
  - Secure
  - Based on modern technologies,
  - Open: Open-source license, well-documented, no GRNET-specifics or hardwired stuff
- Synergies:
  - Customers
  - GEANT & NRENs
  -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

FoD Operation Overview



FoD Operation Overview

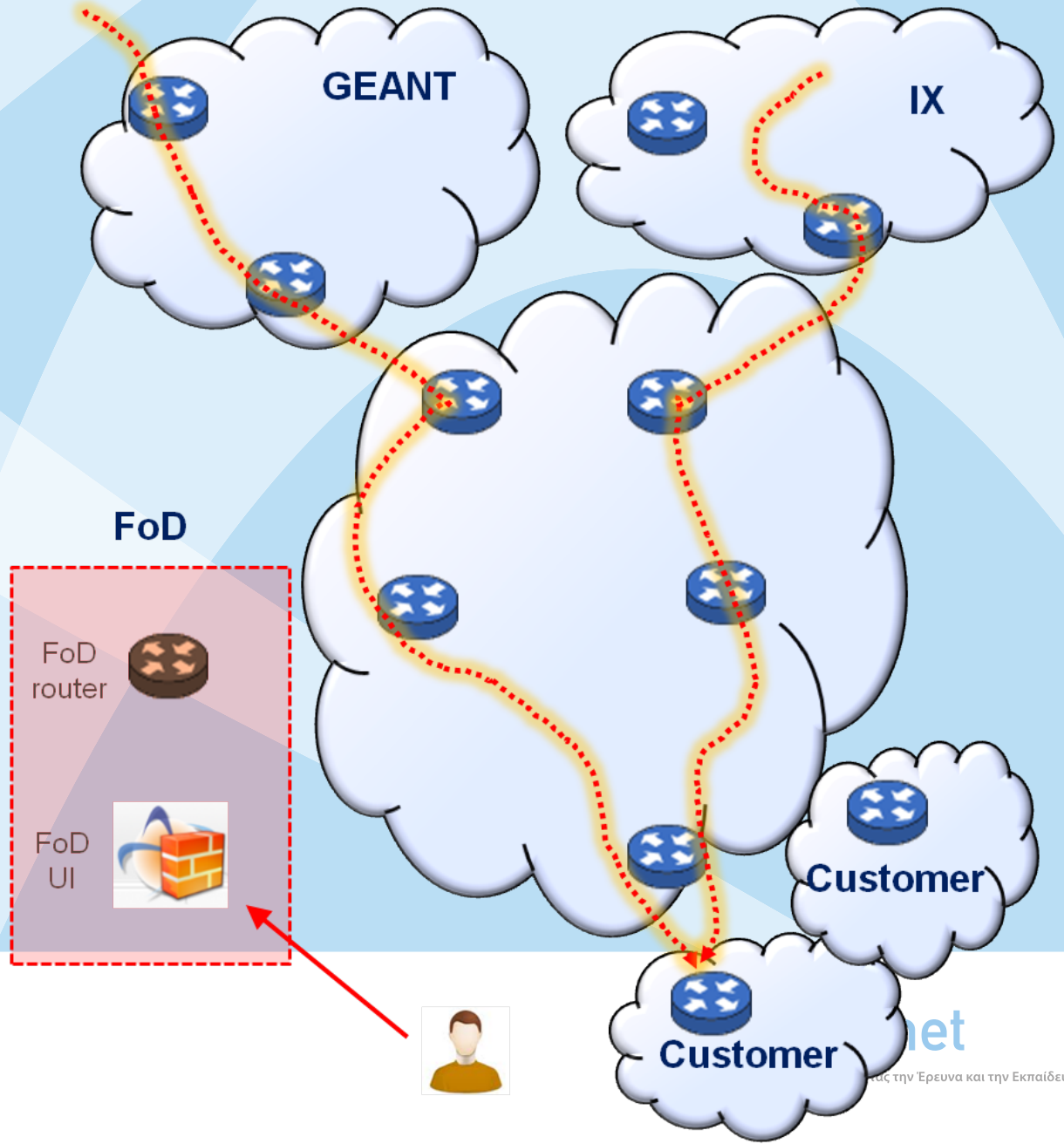
User logs in a web tool and describes flows and actions



FoD Operation Overview

User logs in a web tool and describes flows and actions

Destination validated against user's IP space

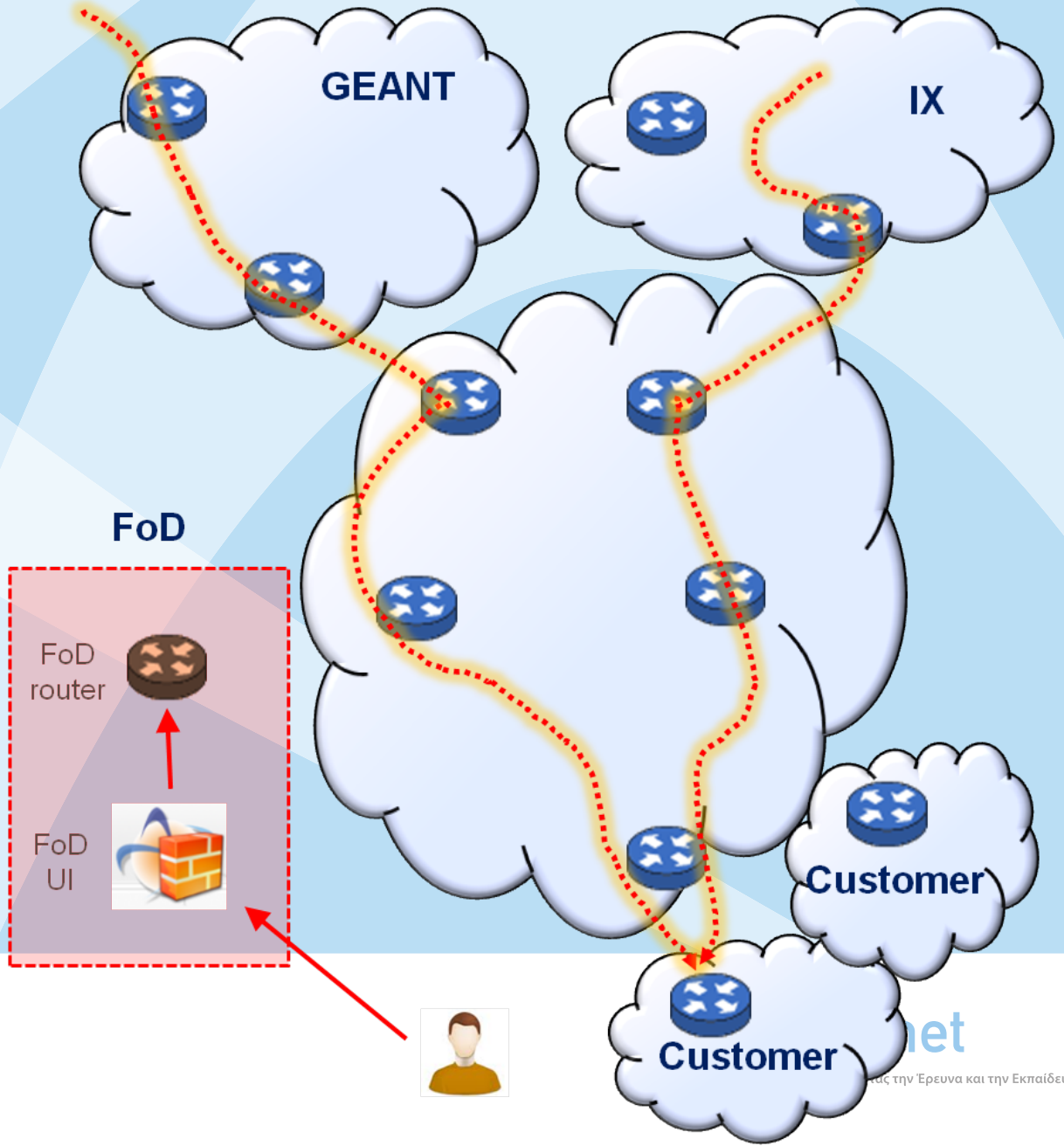


FoD Operation Overview

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



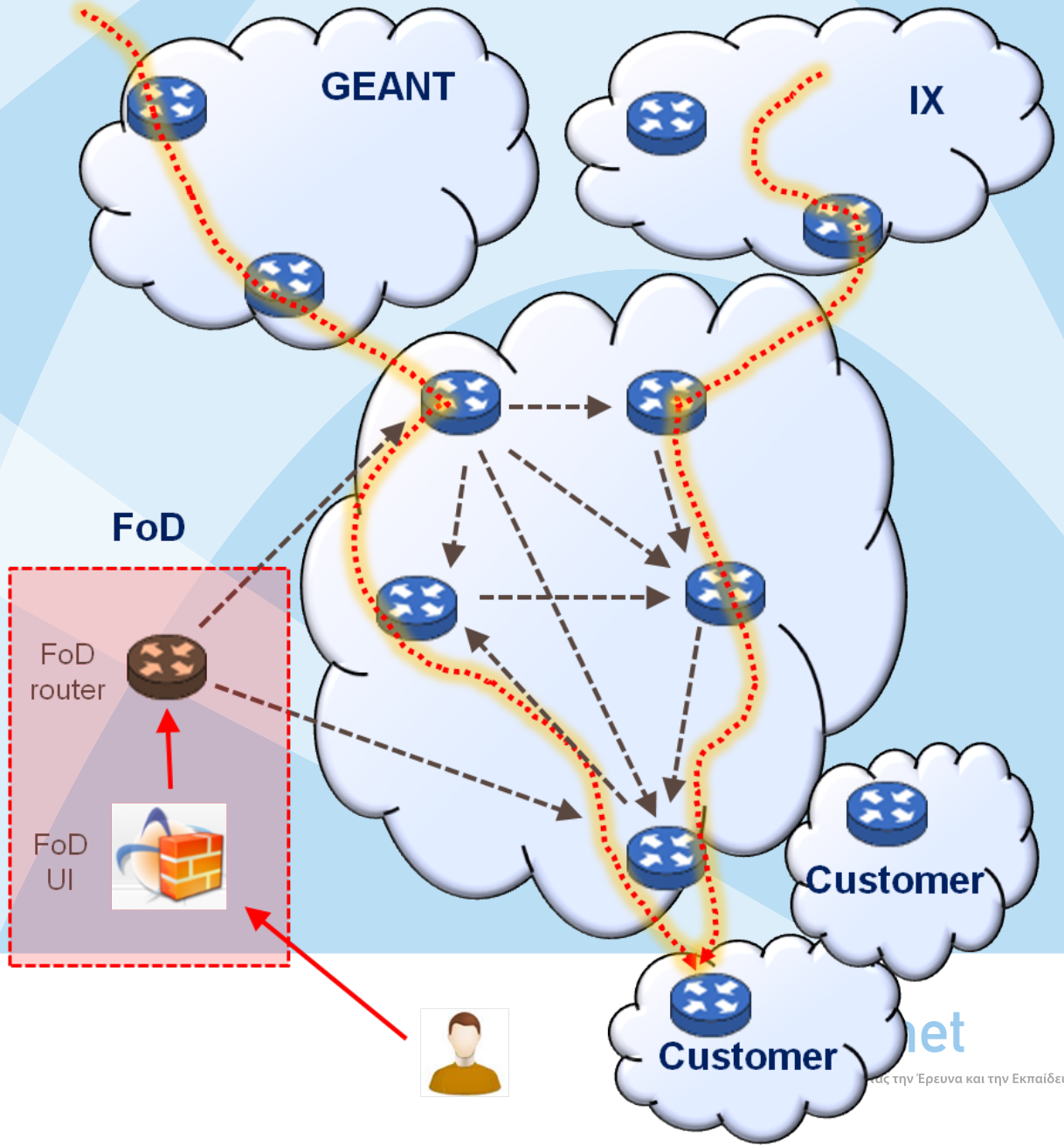
FoD Operation Overview

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 propages the tuples to all GRNET routers.



FoD Operation Overview

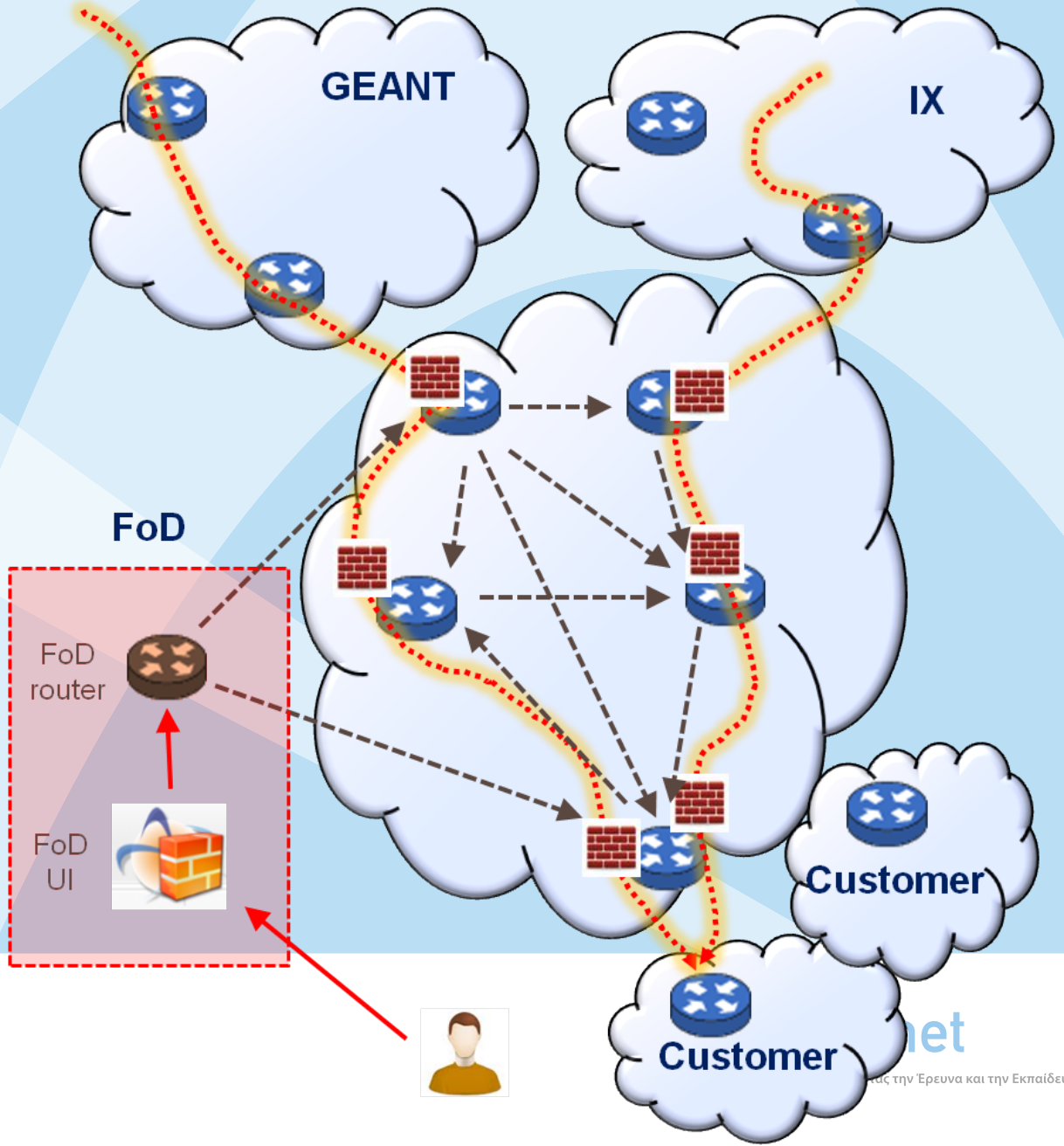
User logs in a web tool and describes flows and actions

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 propages 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

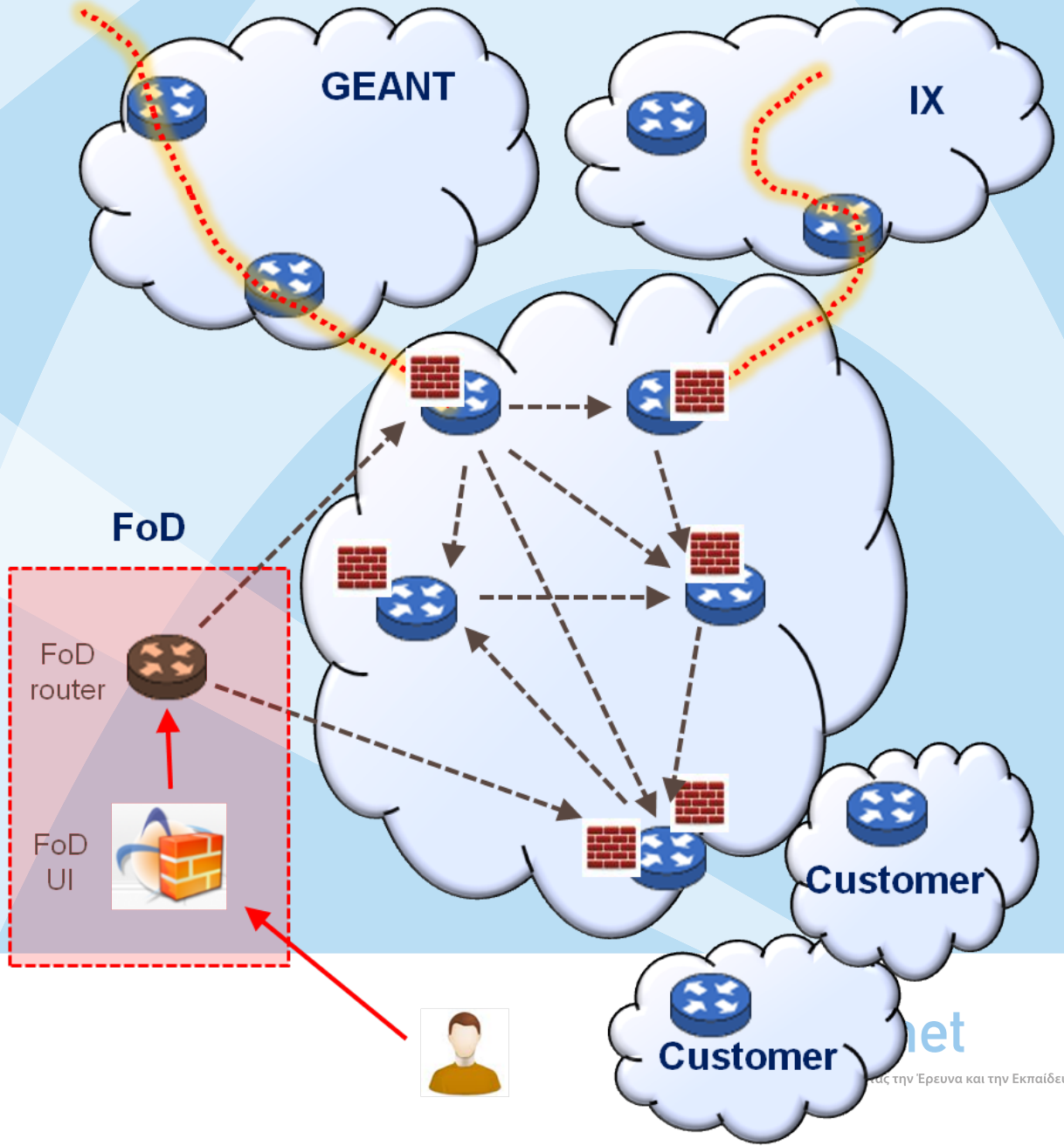
Destination validated against user's IP space

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 propages 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

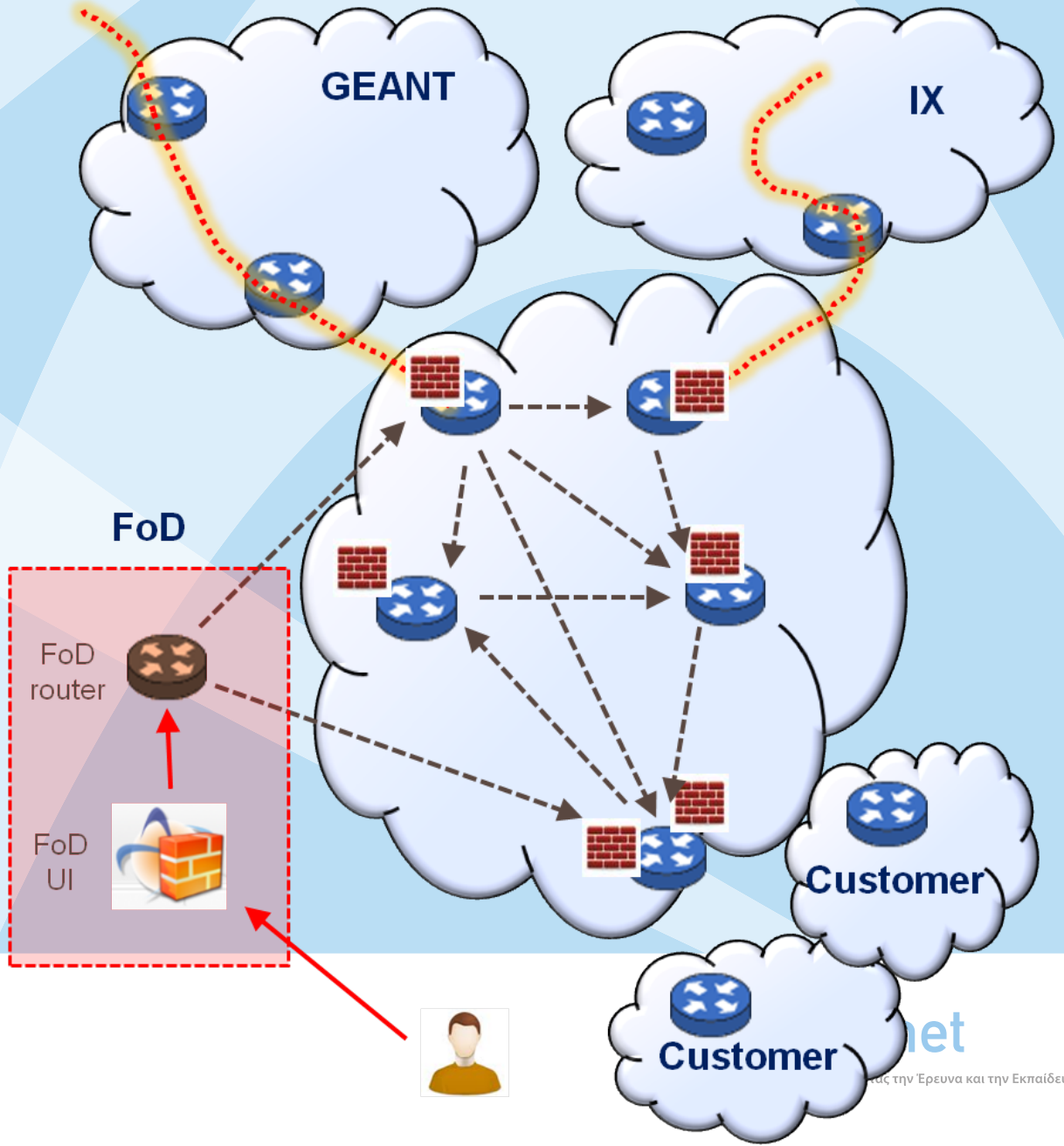
A dedicated router is configured (netconf) to advertise the route via BGP flowspec

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

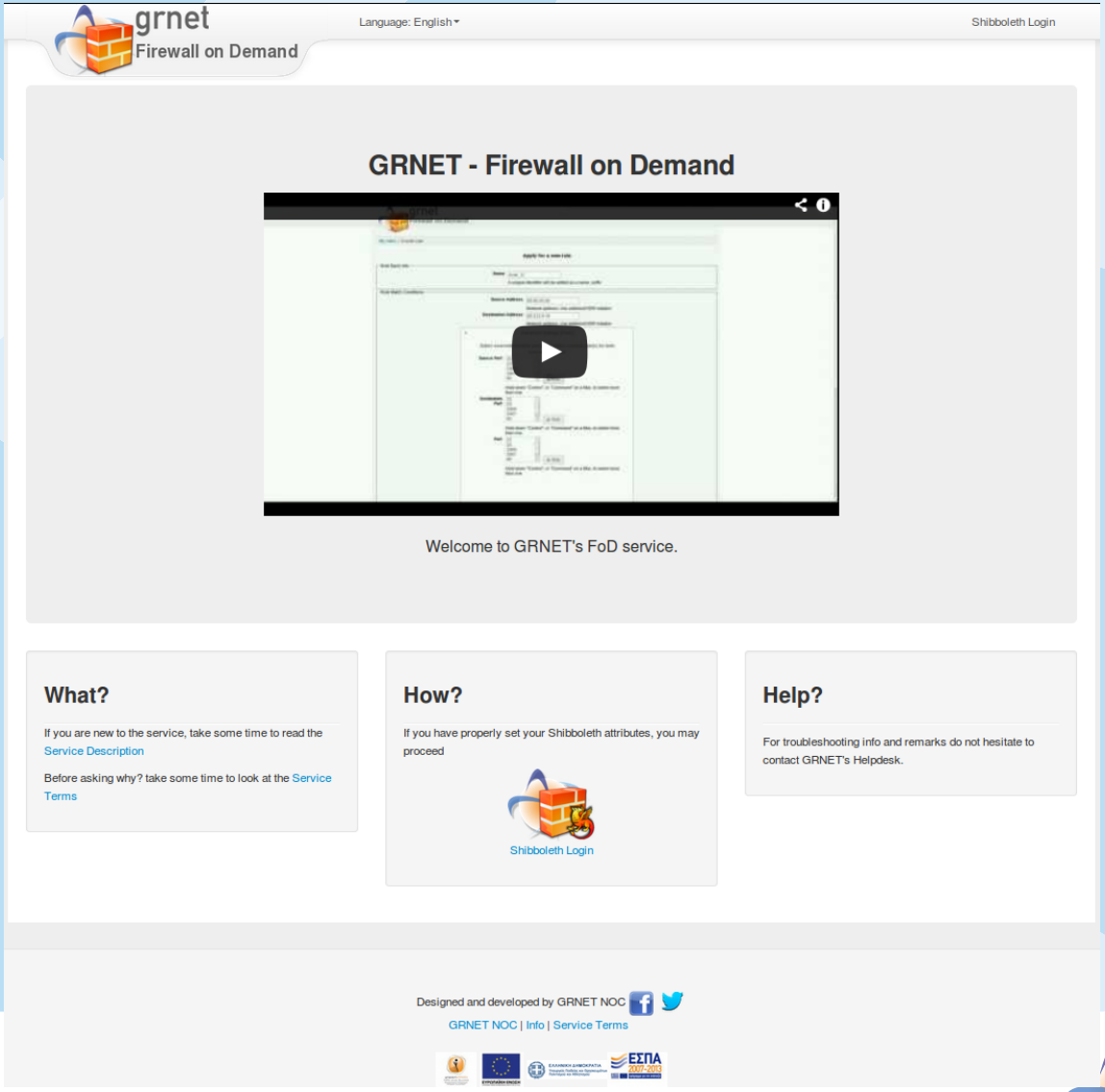
Dynamic firewall filters are implemented on all routers

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

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

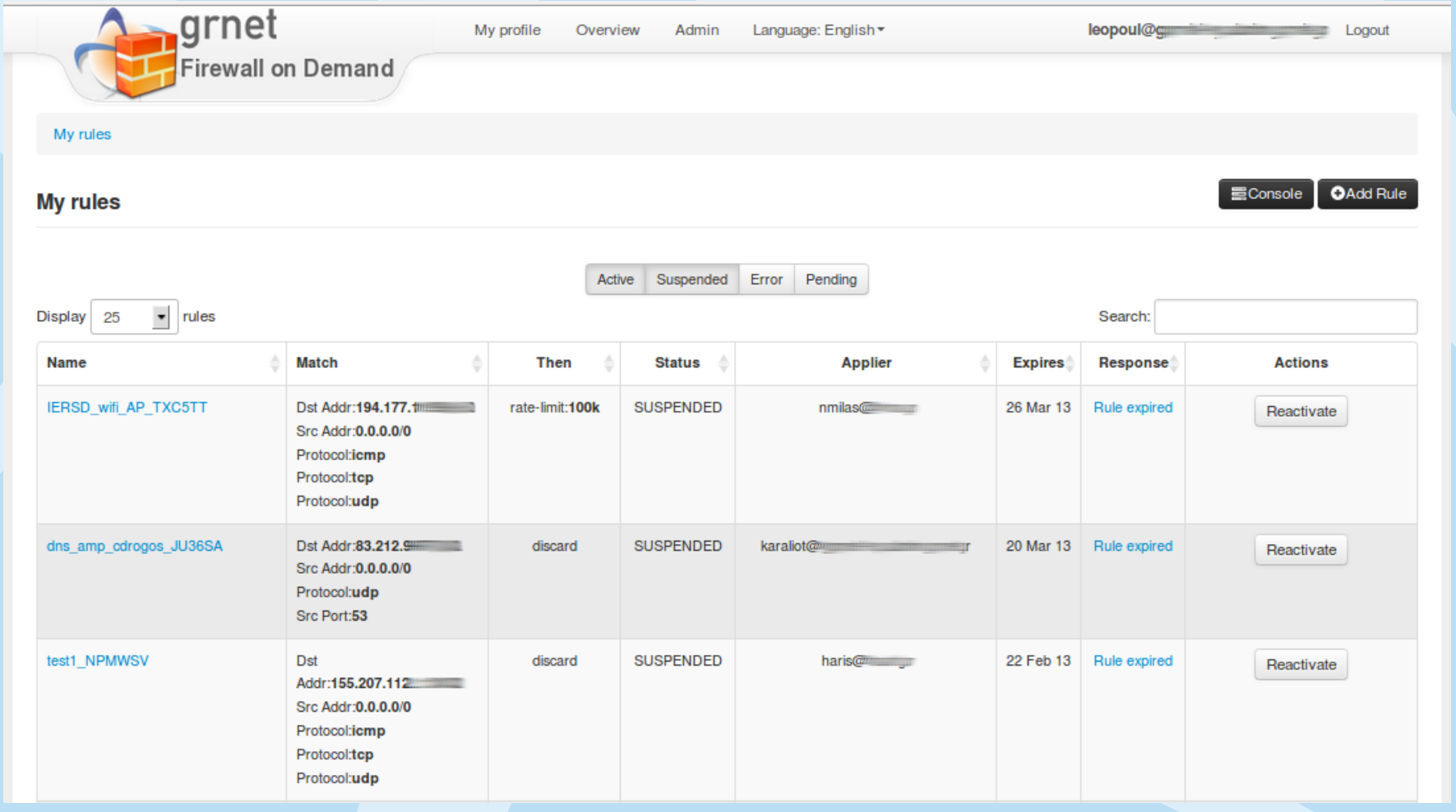


User Interface #1

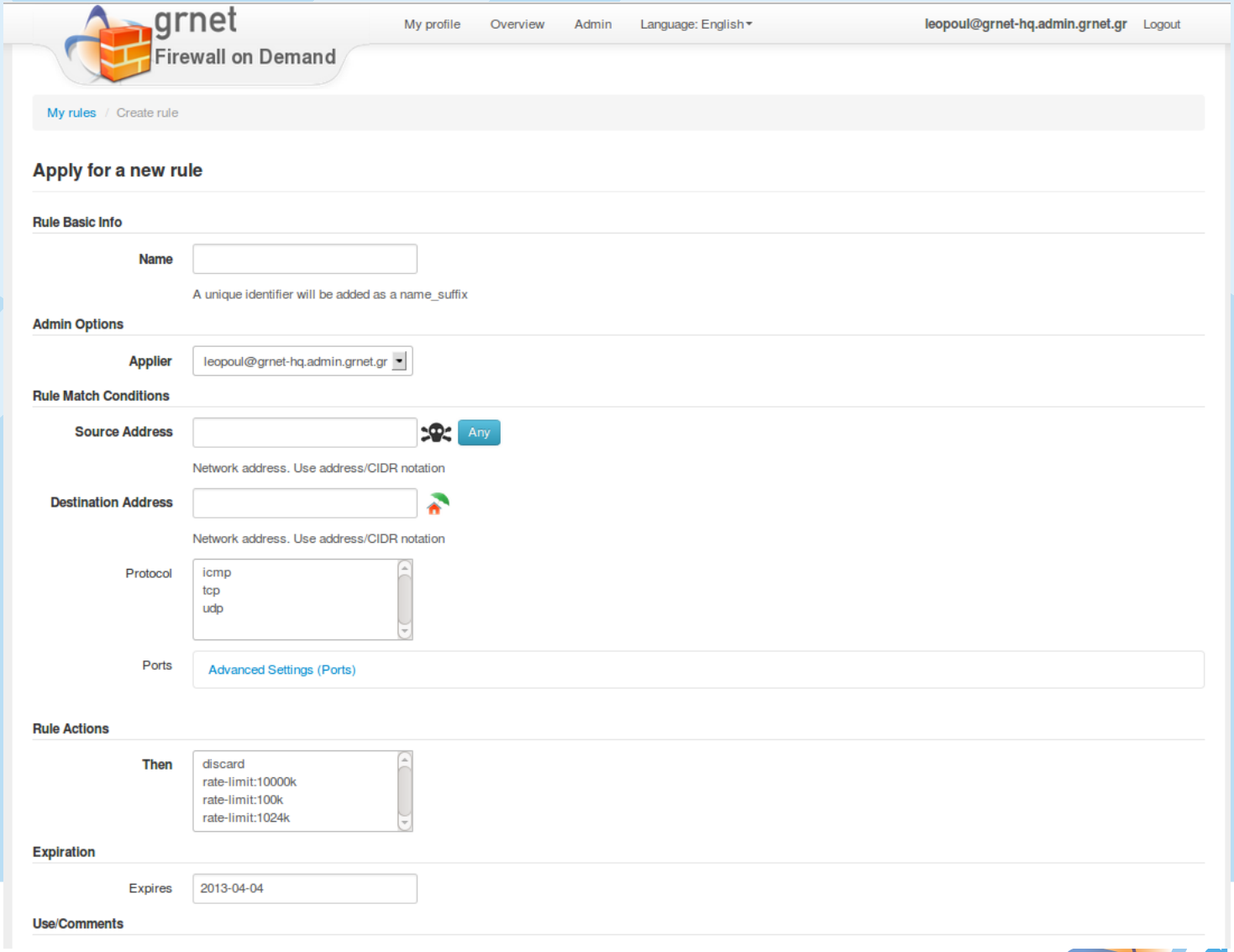


grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

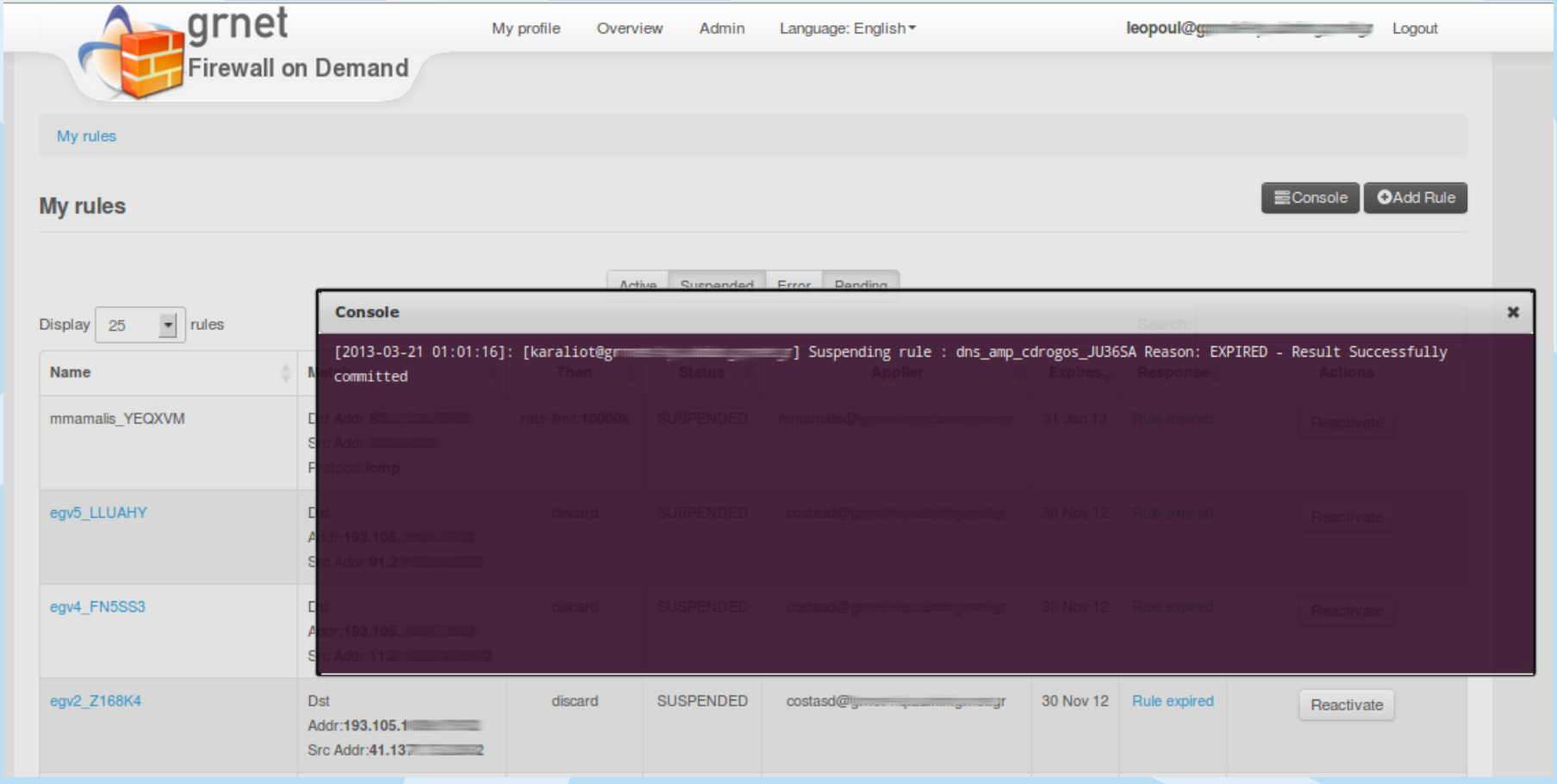
User Interface #2



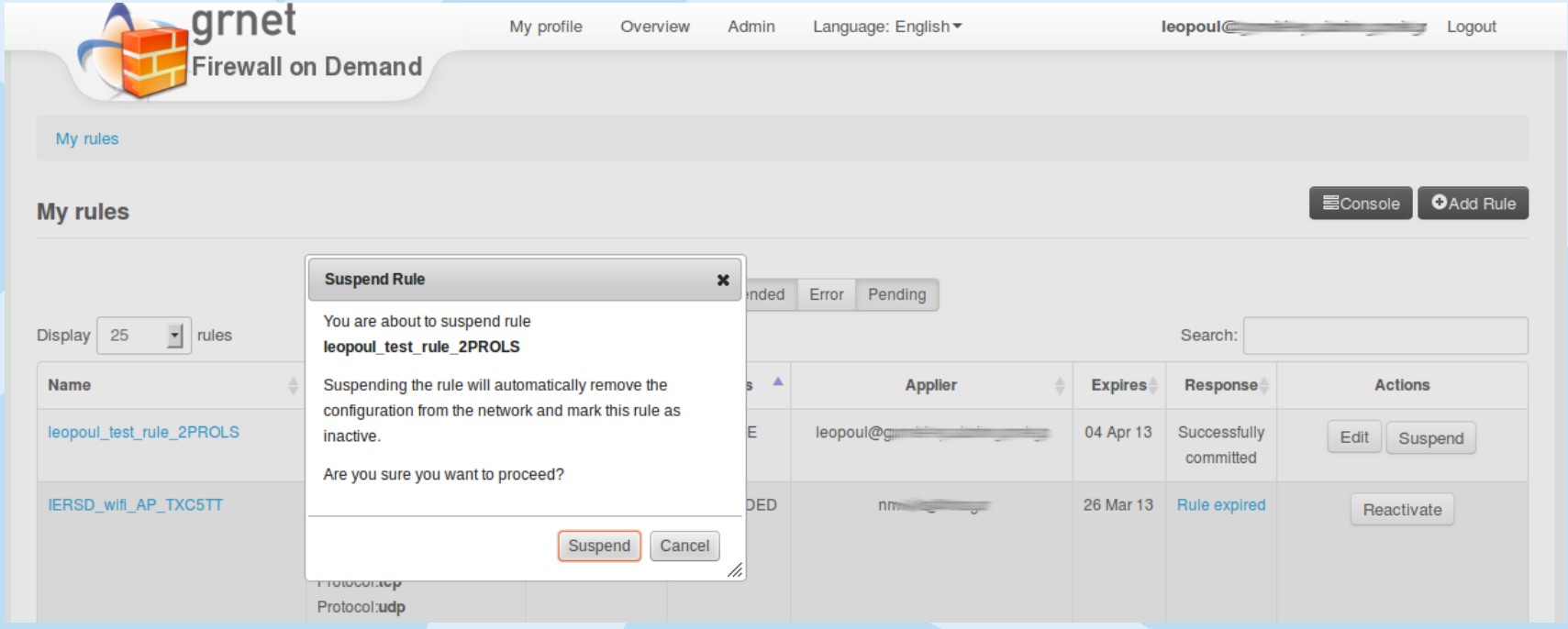
User Interface #3



User Interface #4

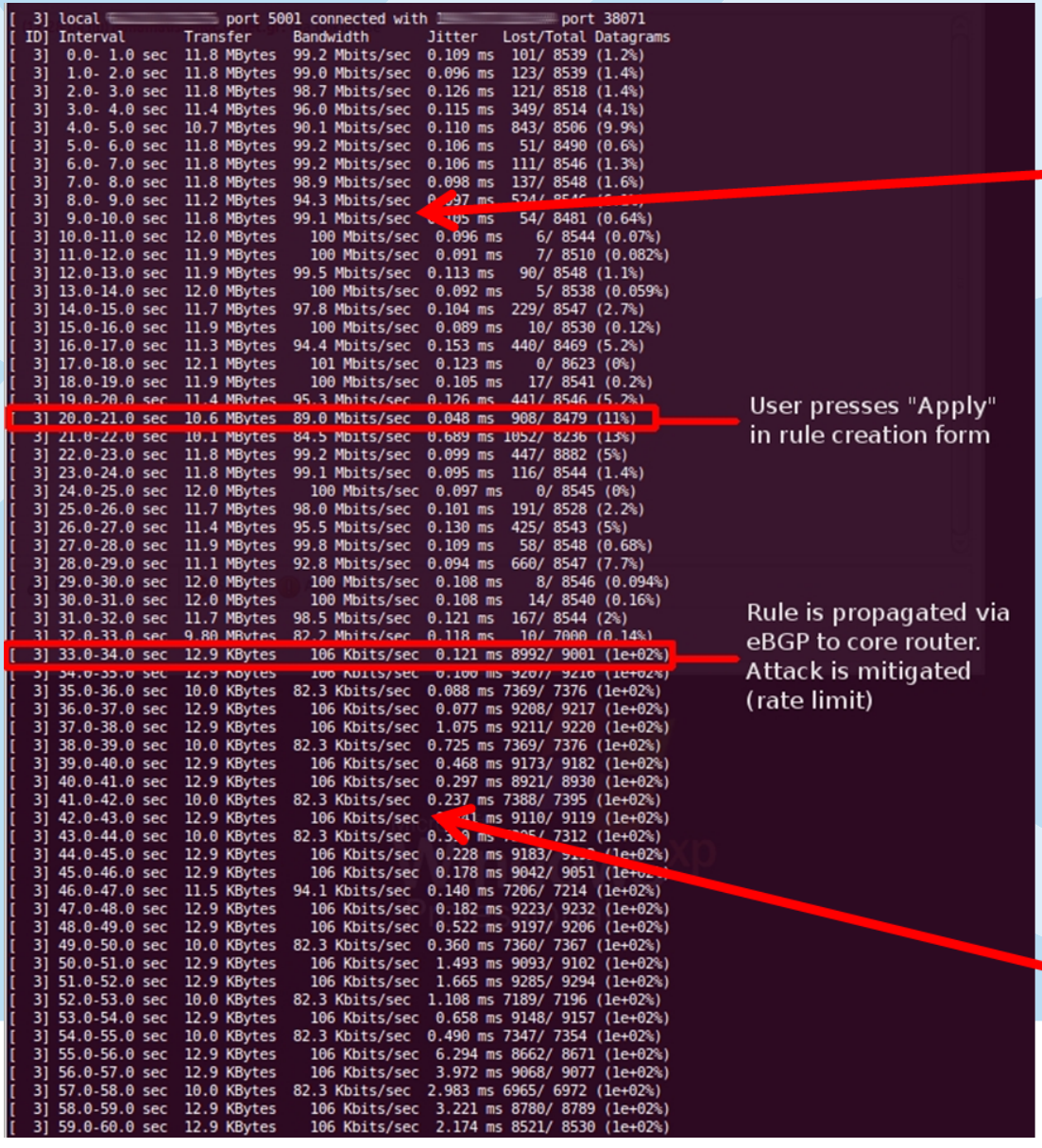


User Interface #5



grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Demo (iperf simulated attack)



A 100Mbps attack

User presses "Apply" in rule creation form

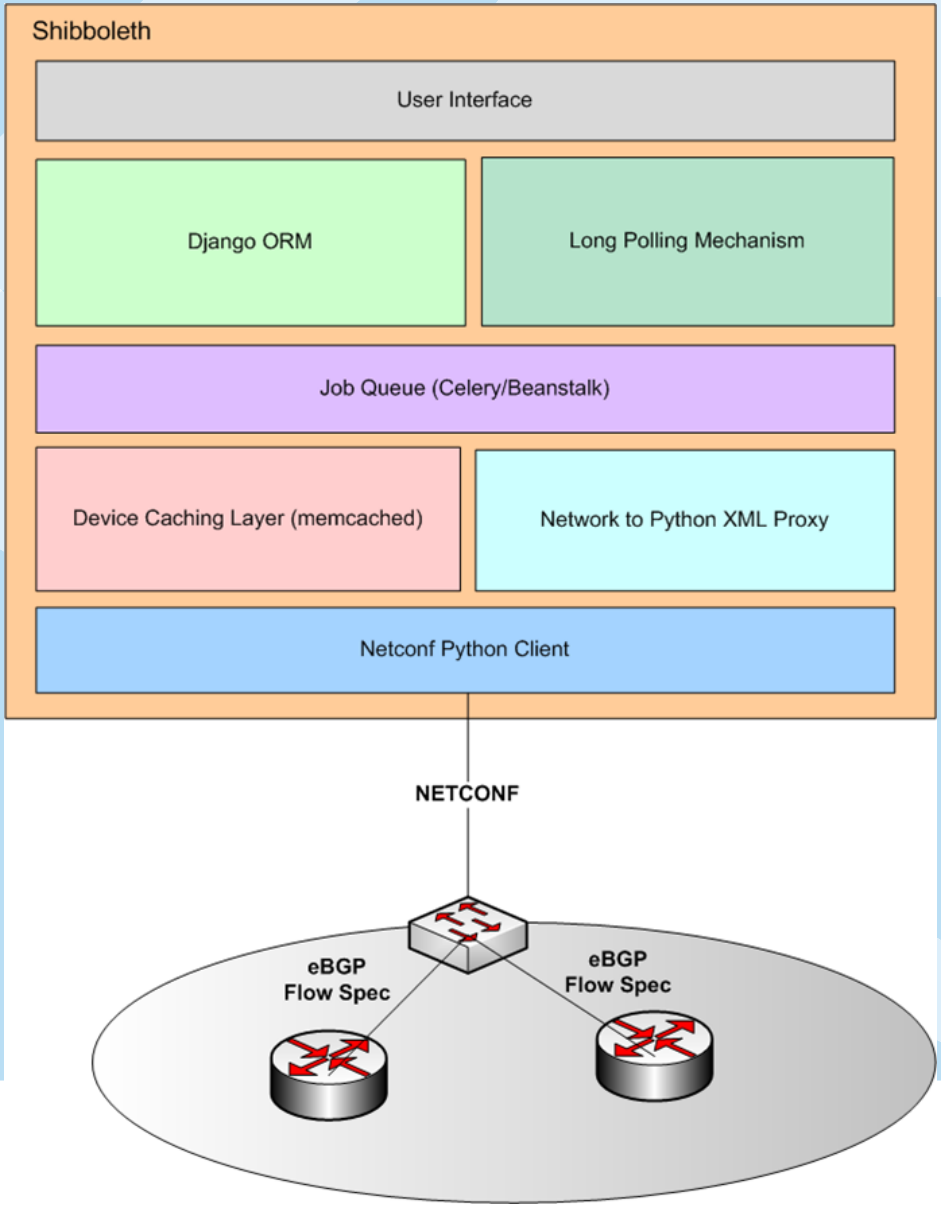
Typically less than 15 seconds

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

Flow limited to 100Kbps

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

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
  - nxpy: Network XML to python classes proxy
    - Dev & maint by GRNET NOC delevoper (Leonidas Poulopoulos)
  - Ncclient: python netconf client (ncclient)
    - Maintained by GRNET NOC delevoper (Leonidas Poulopoulos)
  - 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

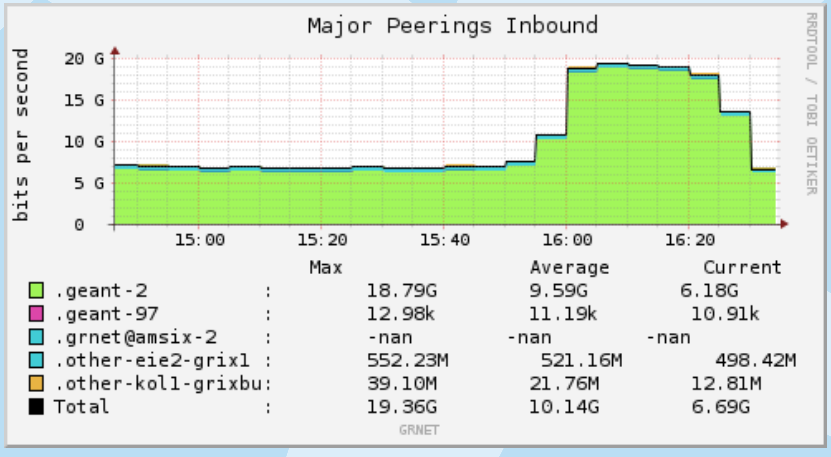
Information Flow

- 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

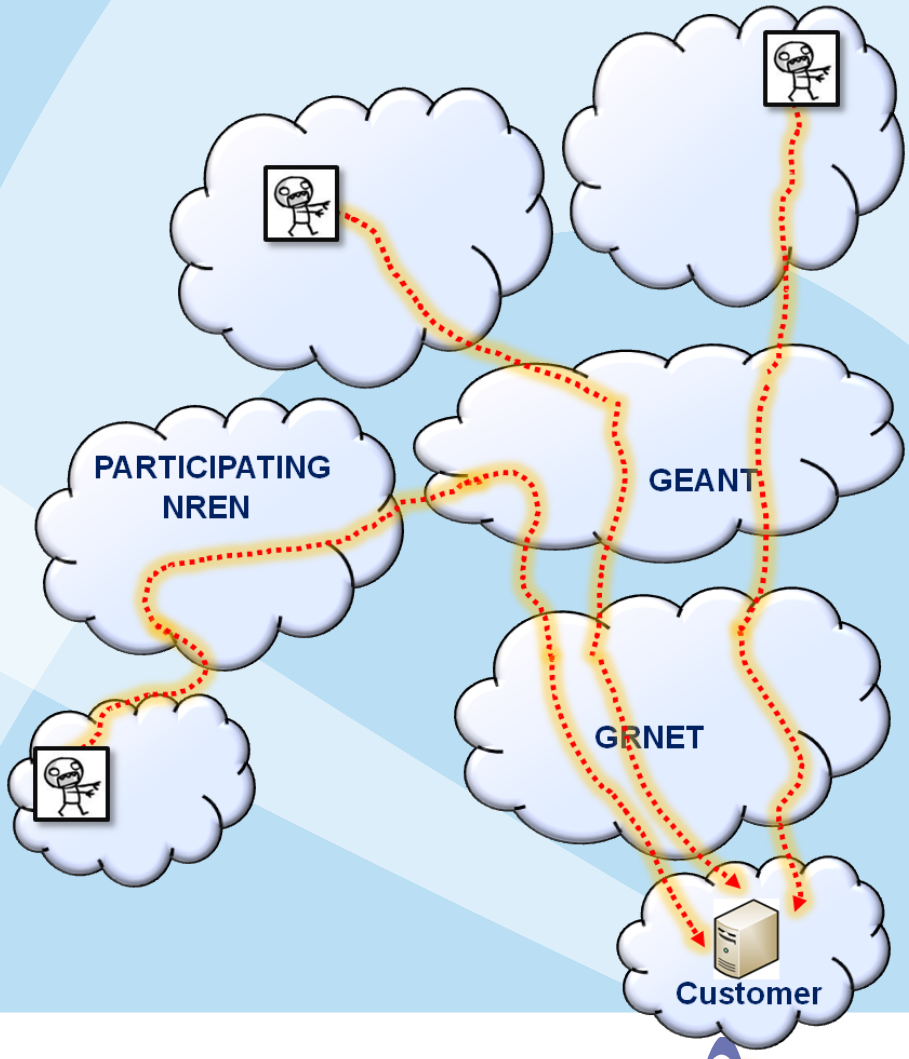
Status

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

- Source code:
  - http://code.grnet.gr/

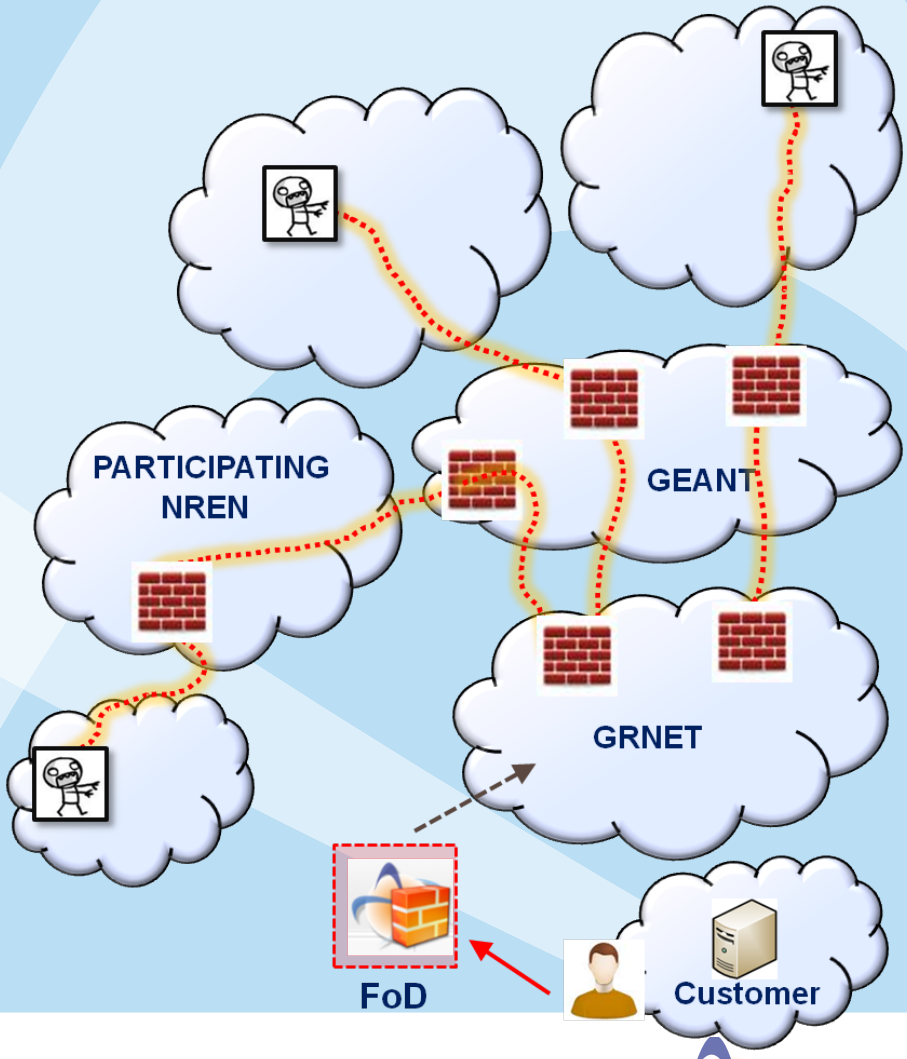
grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Expanding the service to the GEANT community



grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Expanding the service to the GEANT community

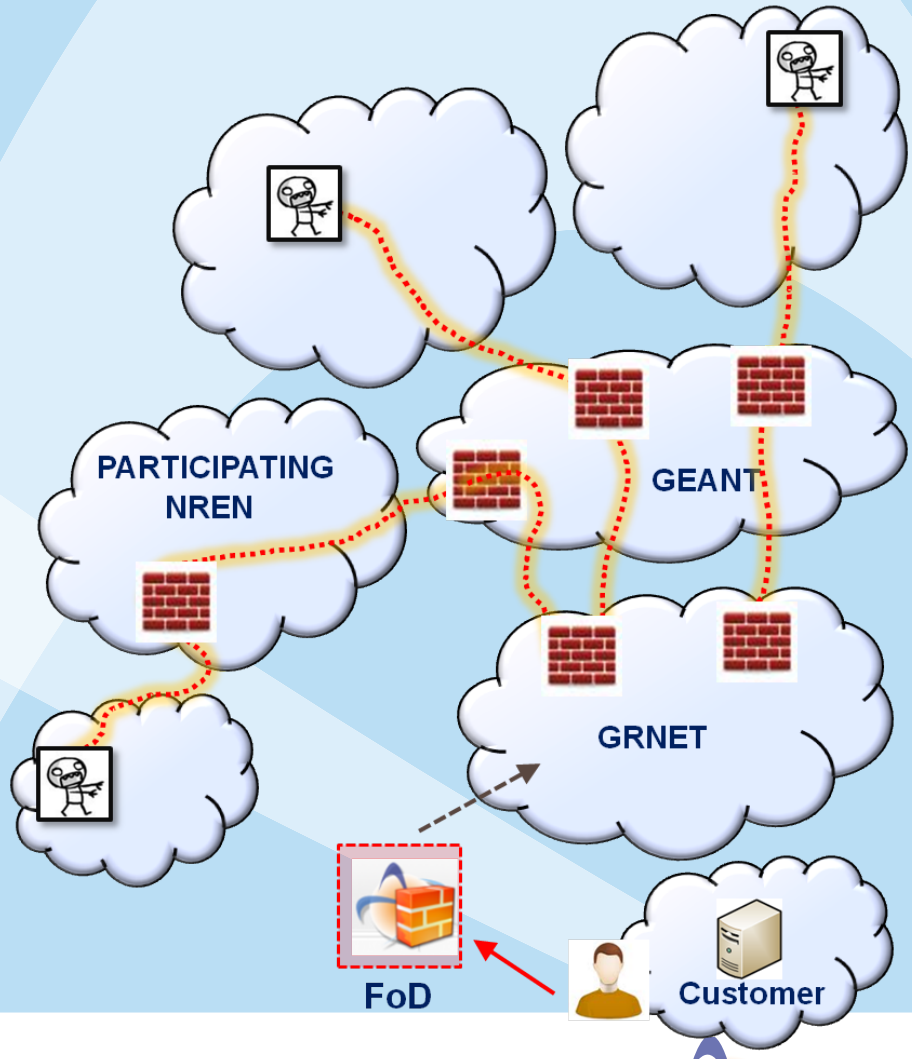


grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Expanding the service to the GEANT community

Phase 1: GEANT participation

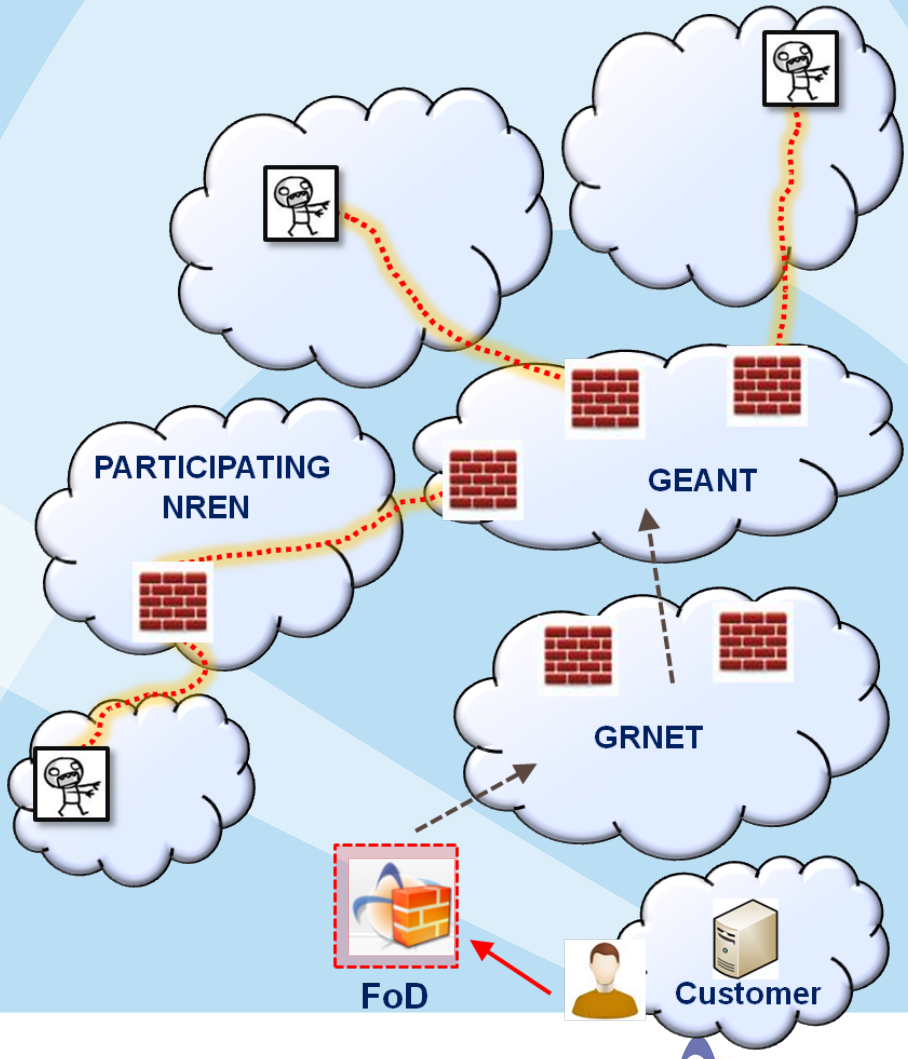
- Routers accept BGP flowspec NLRI
- Establish BGP peerings with GRNET (protected by route-maps)



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



grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

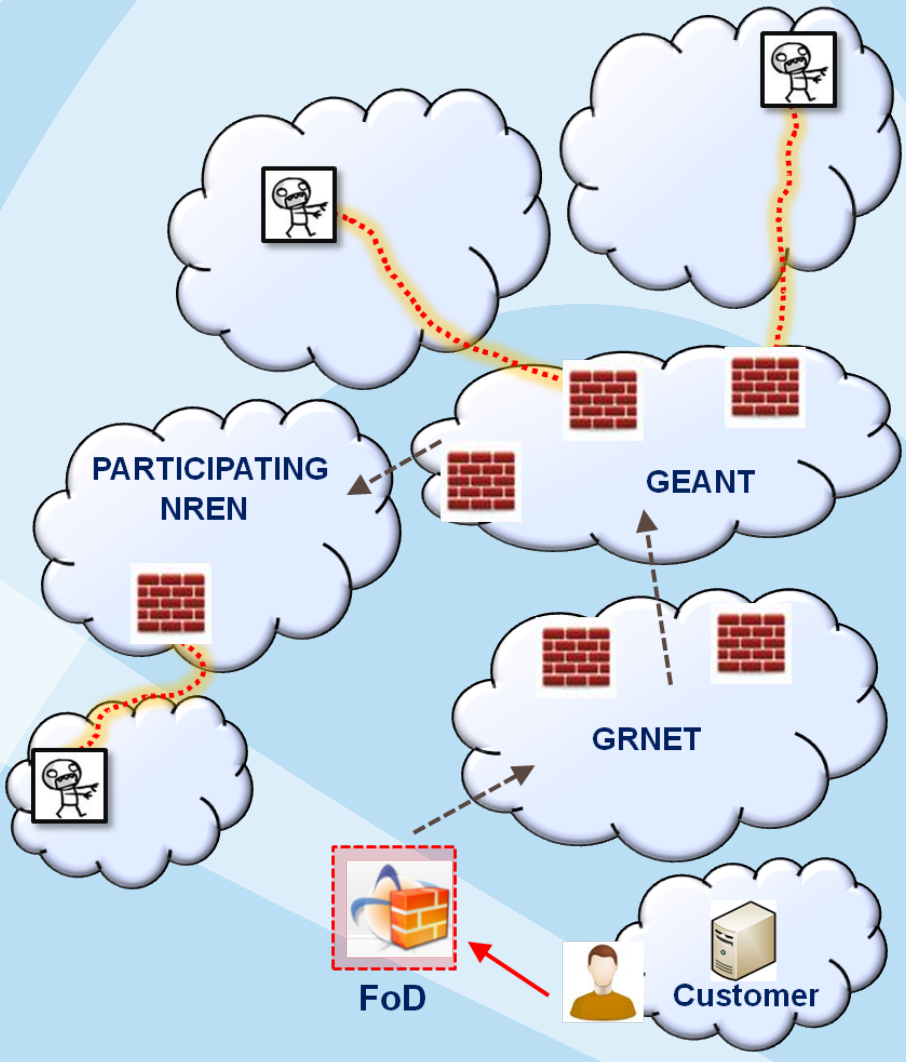
Expanding the service to the GEANT community

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



grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση

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 ommited)
- DB: customers $\rightarrow$ IP space (auth)
  - whois $\rightarrow$ 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 Poulopoulos, Michalis Mamalis & Andreas Polyrakis

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


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


Follow: https://twitter.com/grnetnoc

grnet
Διασυνδέοντας την Έρευνα και την Εκπαίδευση