



# GÉANT

ASSOCIATION

Networking • Services • People

## Firewall on Demand

Evangelos Spatharas

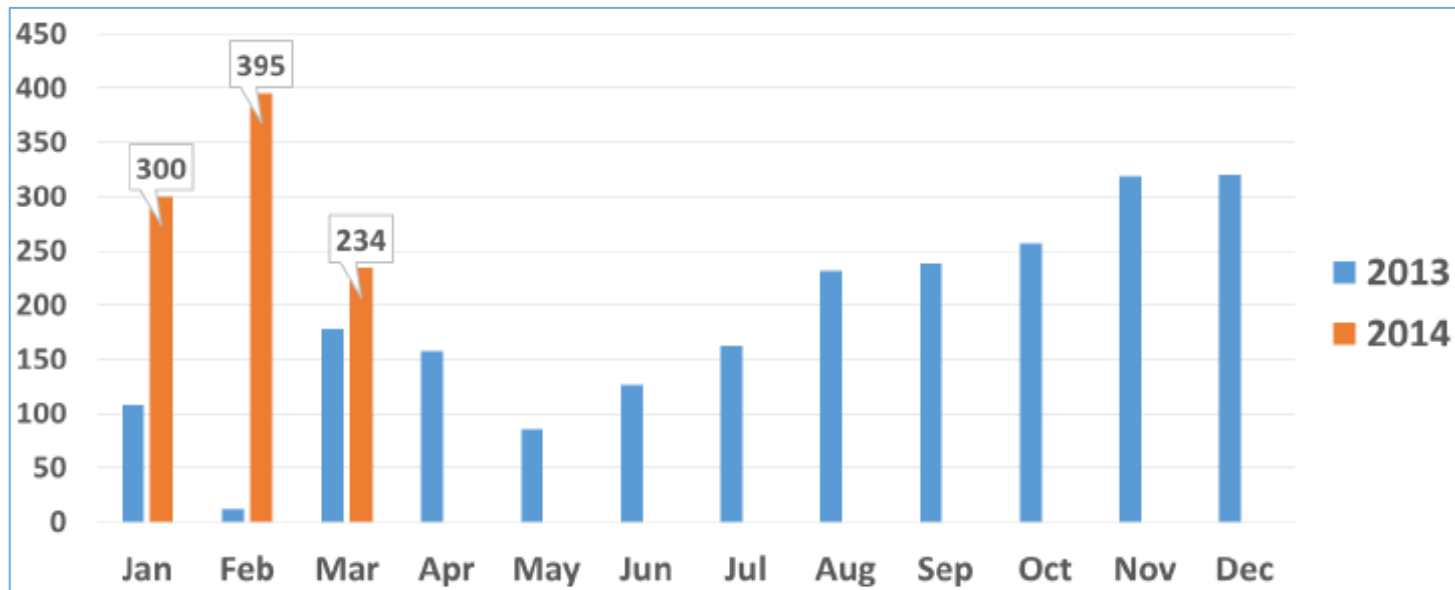
TF-CSIRT/FIRST Meeting

Las Palmas 26 January 2015

- Common network security threats
  - DDoS – statistics, illustration and ramifications
- DDoS Countermeasures
  - Traditional - ACLs
  - Modern BGP Approaches – RTBH/Flowspec
- BGP Flowspec
  - What it is
- From RFC to FoD
  - How it works
  - Security concerns & best practices
- What next
- Q & A

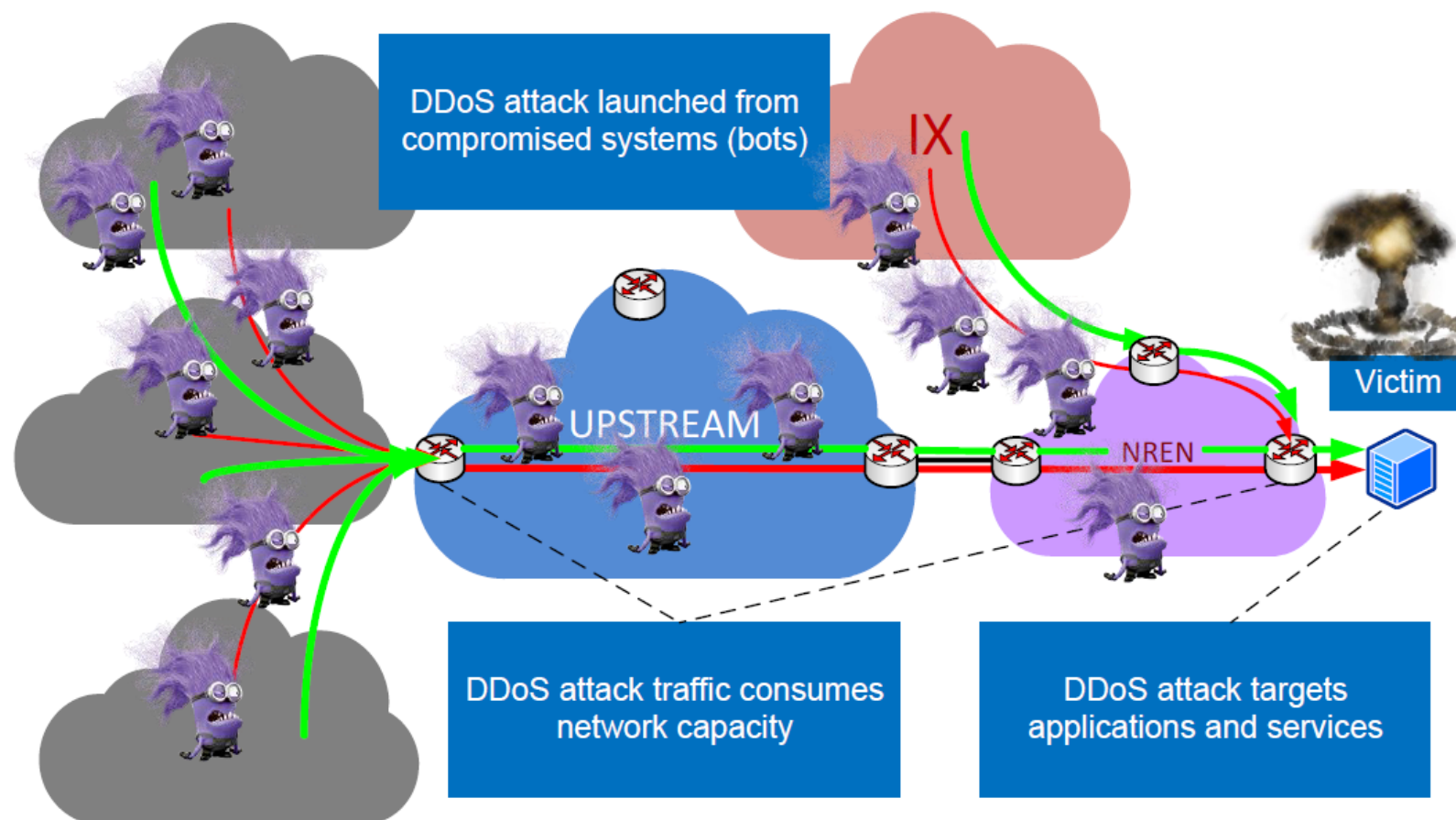
# Network Security Threats

## GEANT



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

# DDoS – High level network view

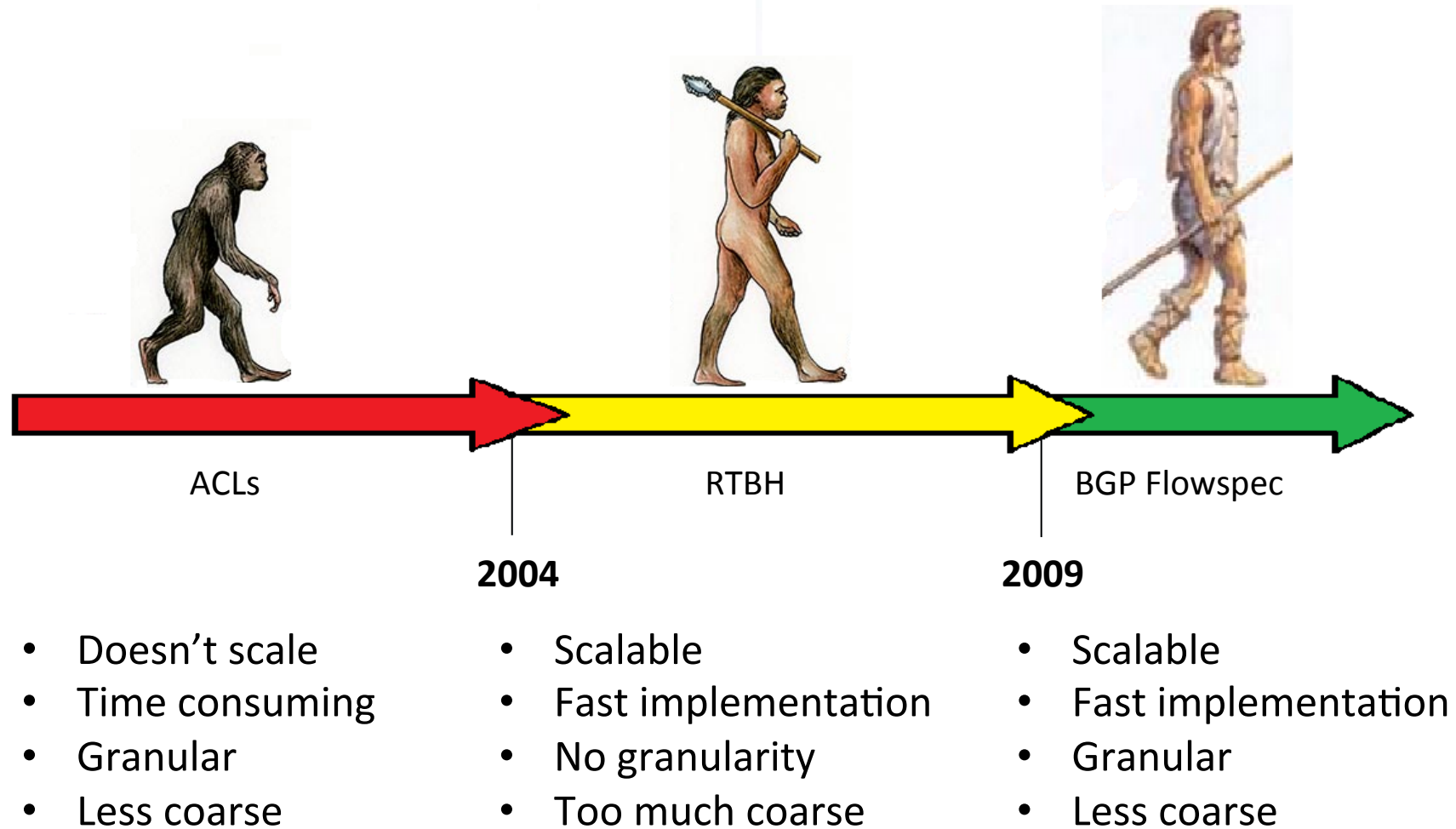


# DDoS – Ramifications

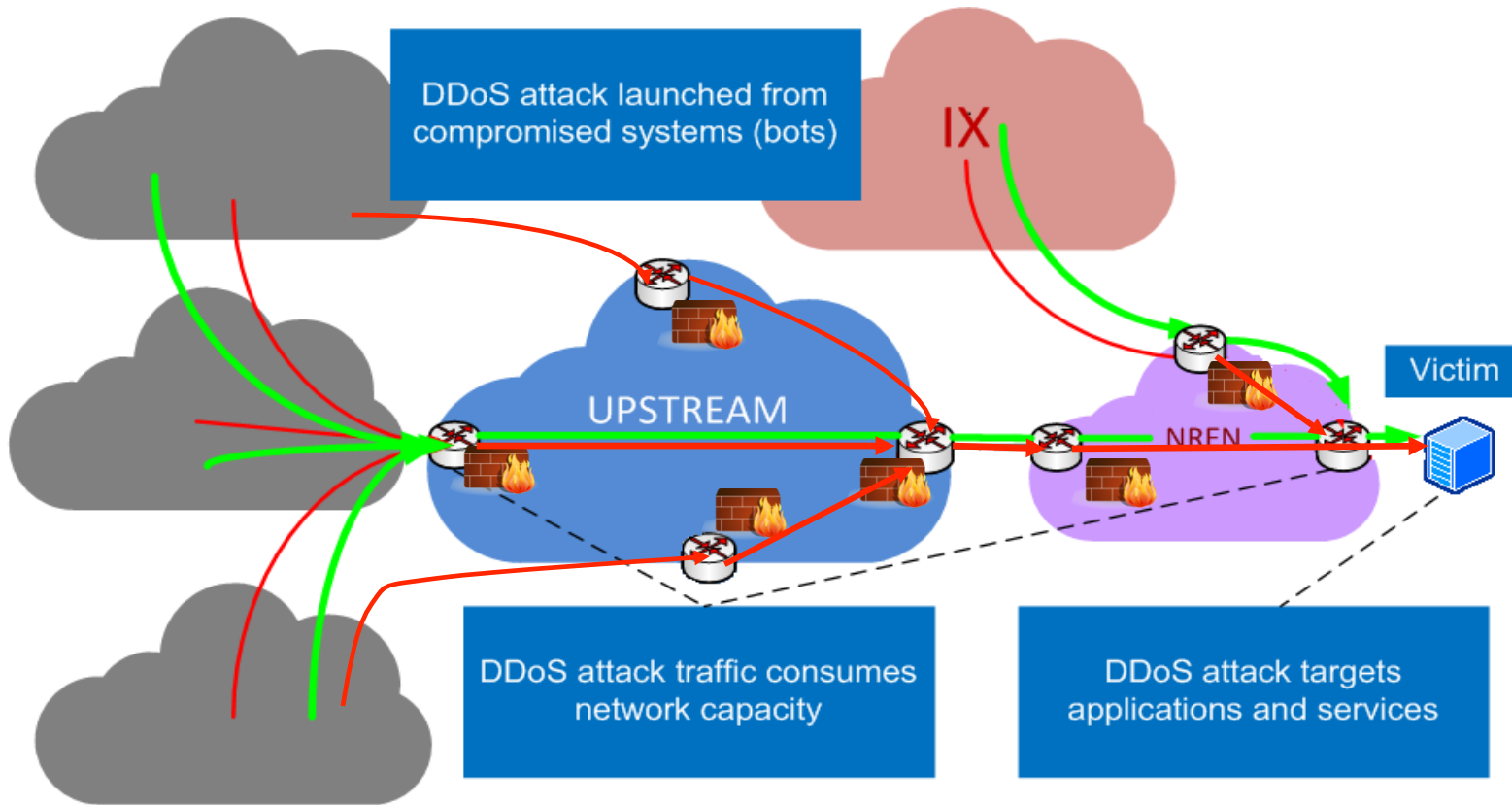
---

- **Network**
  - Performance degradation
  - Services malfunction
  - Outages
- **Staff & Company**
  - Productivity reduction
  - Wasted resources
  - Reputation
  - Profit reduction
- **Clients**
  - Dissatisfaction
  - Change upstream?

# DDoS - Countermeasures



# ACL vs RTBH vs Flowspec



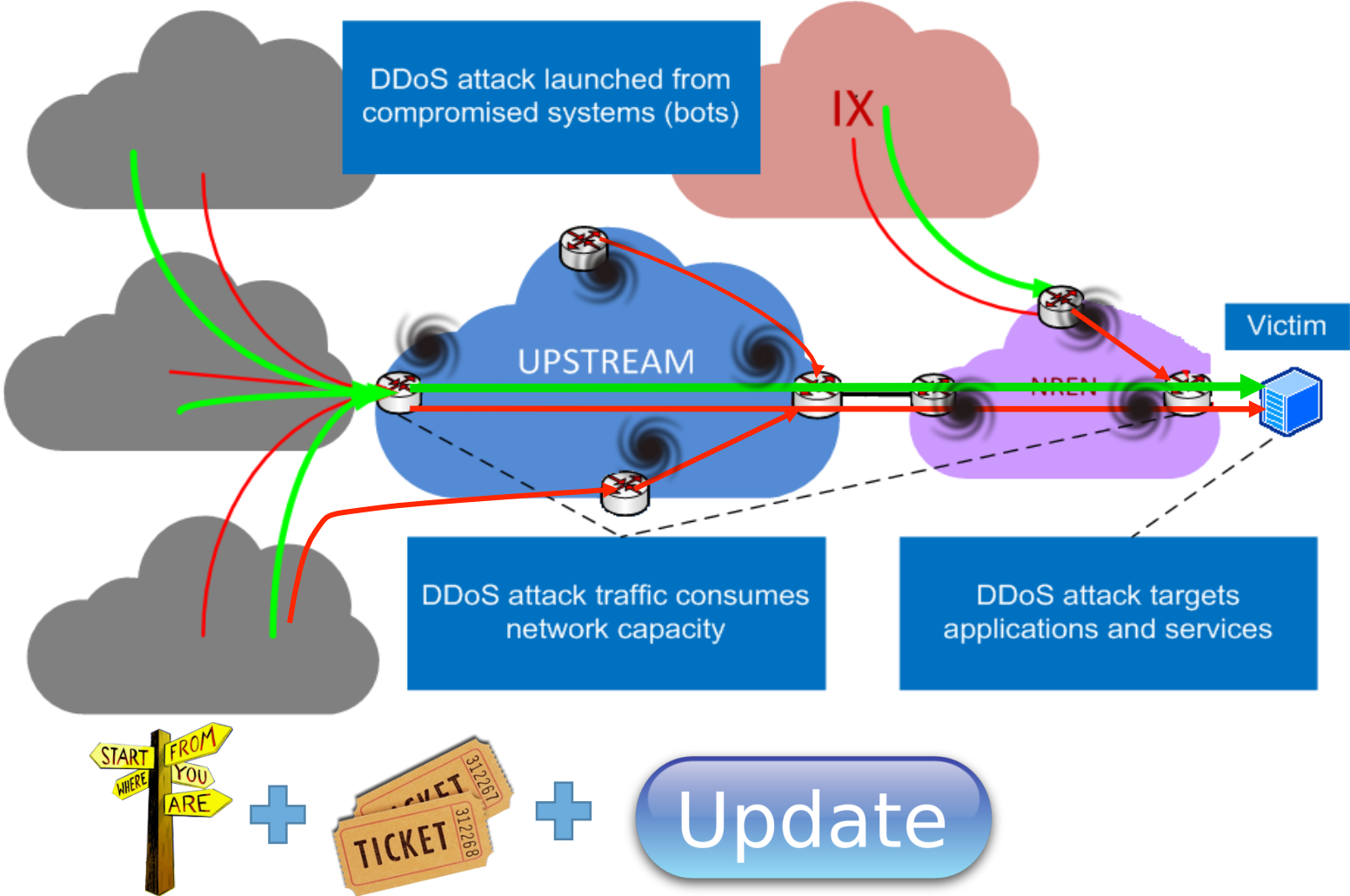
Method	ACL
Efficiency	High
Steps	Many
Legitimate Traffic	Flow
Attacking Traffic	Block
Time	Plenty

— Legitimate traffic

— Attack traffic



# ACL vs RTBH vs Flowspec

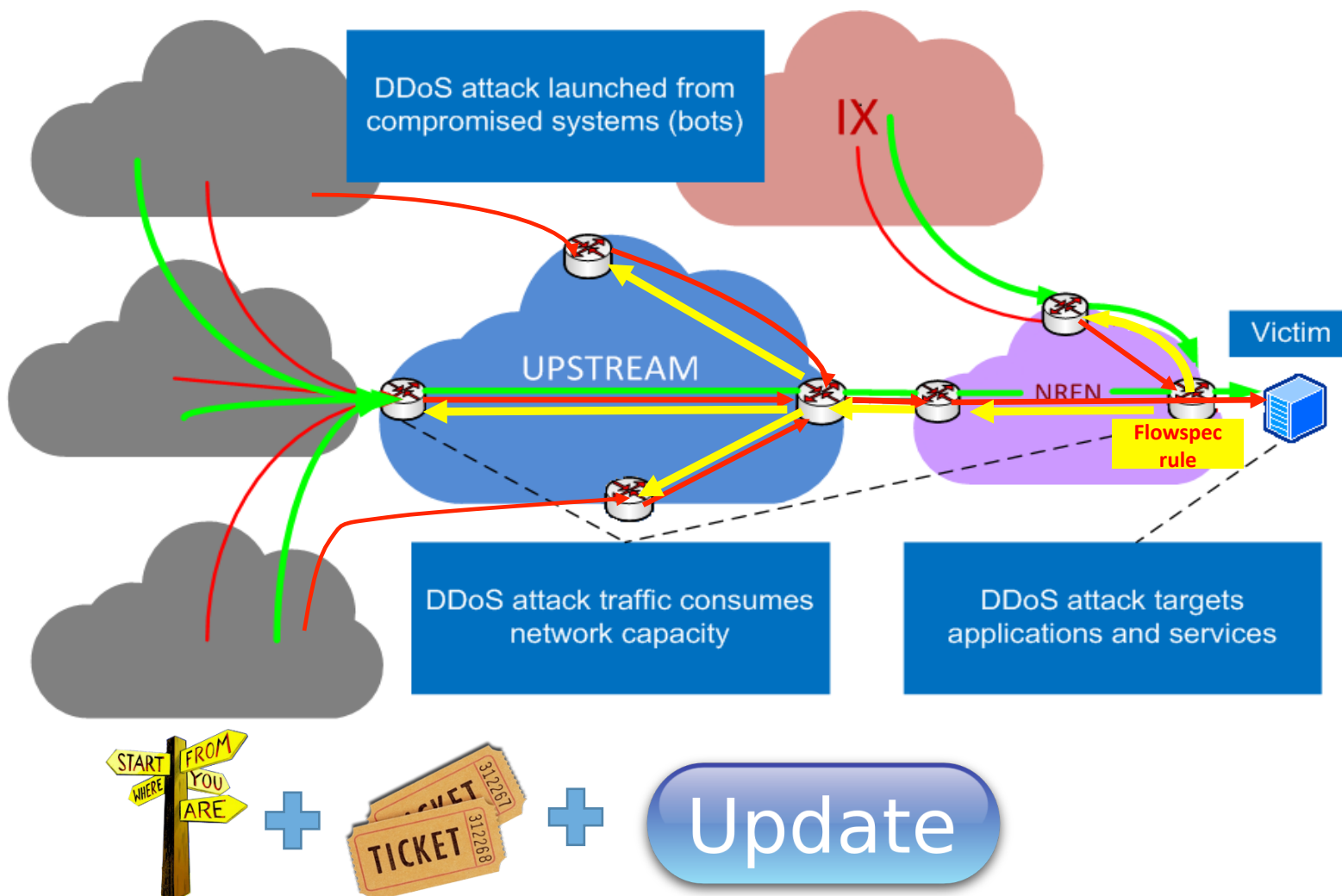


Method	ACL	RTBH
Efficiency	High	Poor
Steps	Many	3
Legitimate Traffic	Flow	Block
Attacking Traffic	Block	Block
Time	Plenty	No

— Legitimate traffic  
— Attack traffic



# ACL vs RTBH vs **Flowspec**



Method	ACL	RTBH	<b>Flowspec</b>
Efficiency	High	Poor	High
Steps	Many	3	3
Legitimate Traffic	Flow	Block	Flow
Attacking Traffic	Block	Block	Block
Time	Plenty	No	No

— Legitimate traffic

— Attack traffic

## BGP Flowspec

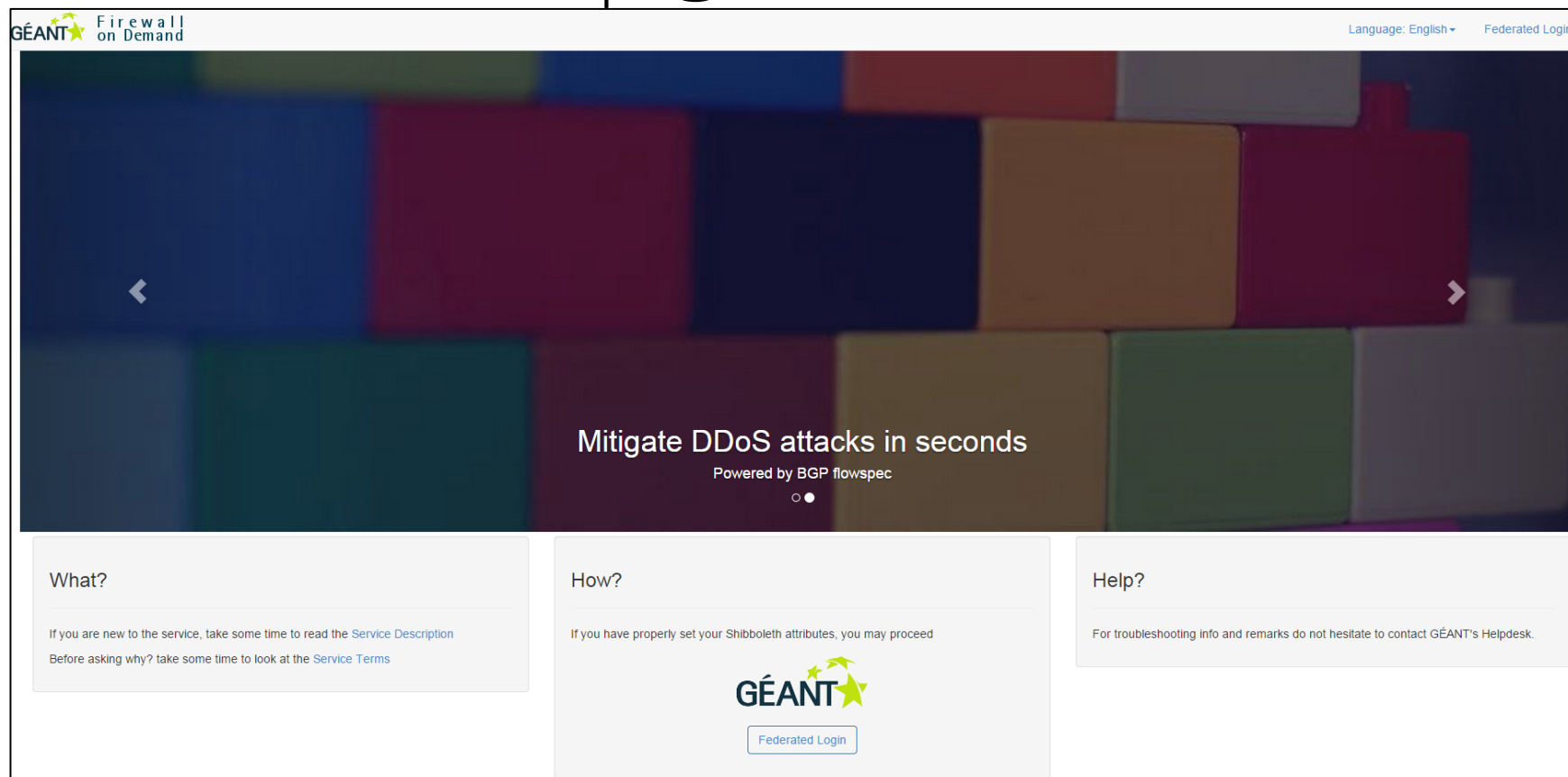
---

- RFC 5575
- Layer 3 and 4 filters are distributed via BGP using a dedicated NLRI
- Currently supported by CISCO, Juniper (only IPv4) and others..
- Match
  - Src/dst prefix
  - Src/dst port
  - ICMP type/code
  - Packet size
  - TCP/UDP protocols
  - TCP flags
  - Others
- Actions
  - Discard
  - Rate-limit
  - Redirect
  - Accept
  - Others

## From RFC to a WEB based tool

# fod.geant.net

- GOOD! Till now all work perfect! ....



Developed and designed by 

Dashl

Rules

Add F

My pr

Timeline - Latest 10

firstrule\_GEANT\_I6W1NM

Last update: Sept. 11, 2014, 3:10 p.m. by leopard:GRNET

Expires: 18 Sep 14

ACTIVE

Dst Addr83.212.9.78/32

Src Addr62.40.30.162/31

Protocolsicmp, tcp, udp

SrcPorts80, 8080

Thenrate-limit 100k

Edit

Deactivate

Firewall Rules

20 records per page

ACTIVE

PENDING

ERROR

DEACTIVATED

Search:

Previous

1

Next

Showing 1 to 1 of 1 entries

Name	Match	Then	Status	Applier	Expires	Response	Actions
firstrule_GEANT_I6W1NM	<div><div>Dst Addr</div><div>Src Addr</div><div>Protocols</div><div>SrcPorts</div></div> <div><div></div><div></div><div>icmp, tcp, udp</div><div>80, 8080</div></div>	rate-limit 100k	ACTIVE	leopard:GRNET	2014-09-18	Successfully committed	<div><div>Edit</div><div>Deactivate</div></div>

Showing 1 to 1 of 1 entries

Previous

1

Next

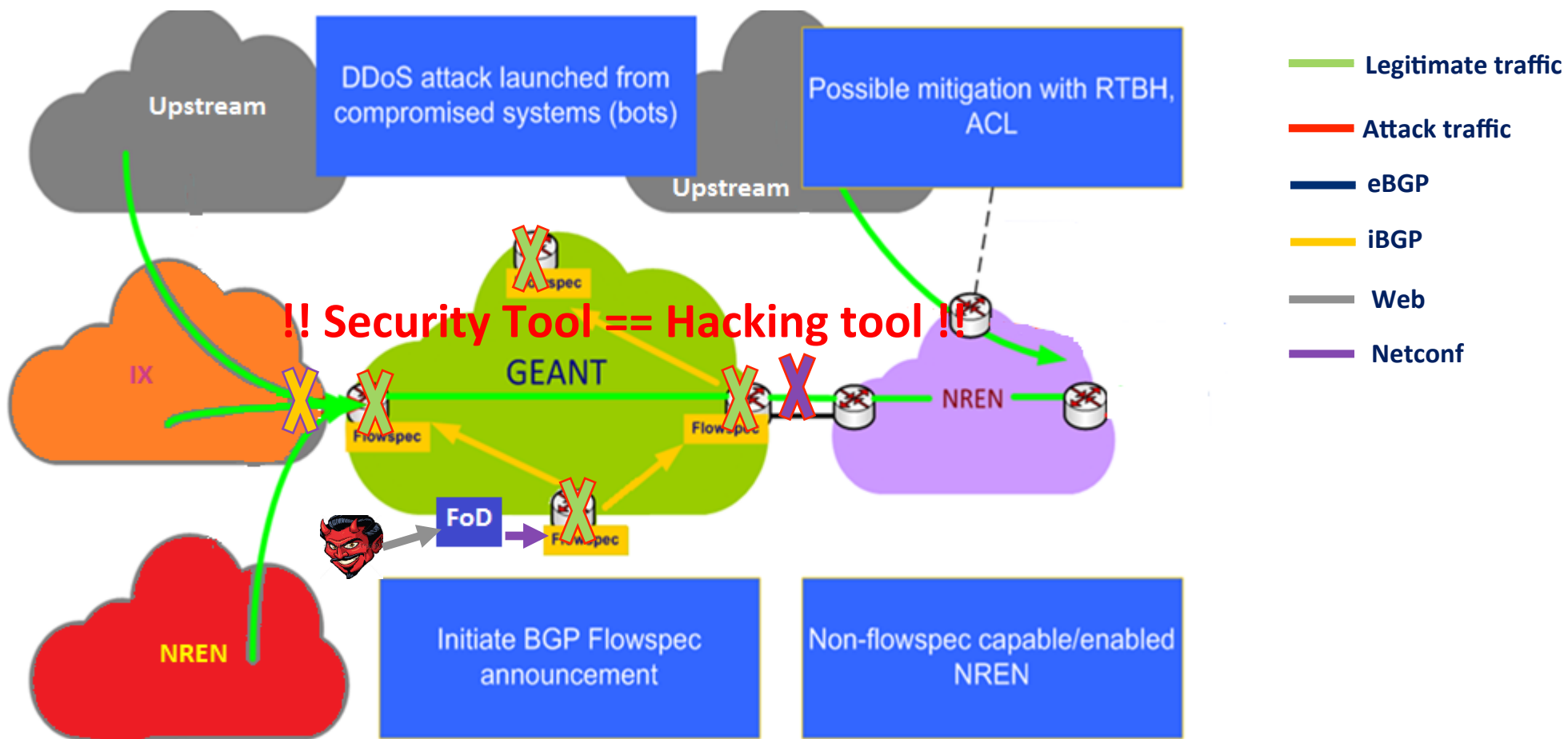
Networking • Services • People | [www.geant.org](http://www.geant.org)

12

# How does it work behind the scenes



## Security Concerns – A hypothetical scenario



# Security Best Practices

---

- **Application level**
  - ✓ NRENs can only block traffic that destined towards their IP space
  - ✓ A user can only filter up to /29 subnet blocks
  - ✓ Only explicitly defined NOC admins have access rights to FoD application
  - ✓ Flowspec rules are automatically deactivated after one week unless explicitly specified
  - ✓ Logging
- **Network level**
  - ✓ Before a flow route installed on the table, is checked against subnet length
  - ✓ Even an admin user cannot block traffic destined to GEANT routers (via policy)
  - ✓ Reachable only from GEANT/NREN IP space

**Okay! I want to use it!!!**

---

## **Status**

**Currently: Installing/configuring the platform**

**Next: Running final pilot – February 2015 onwards**

**In production: Before end of March 2015**

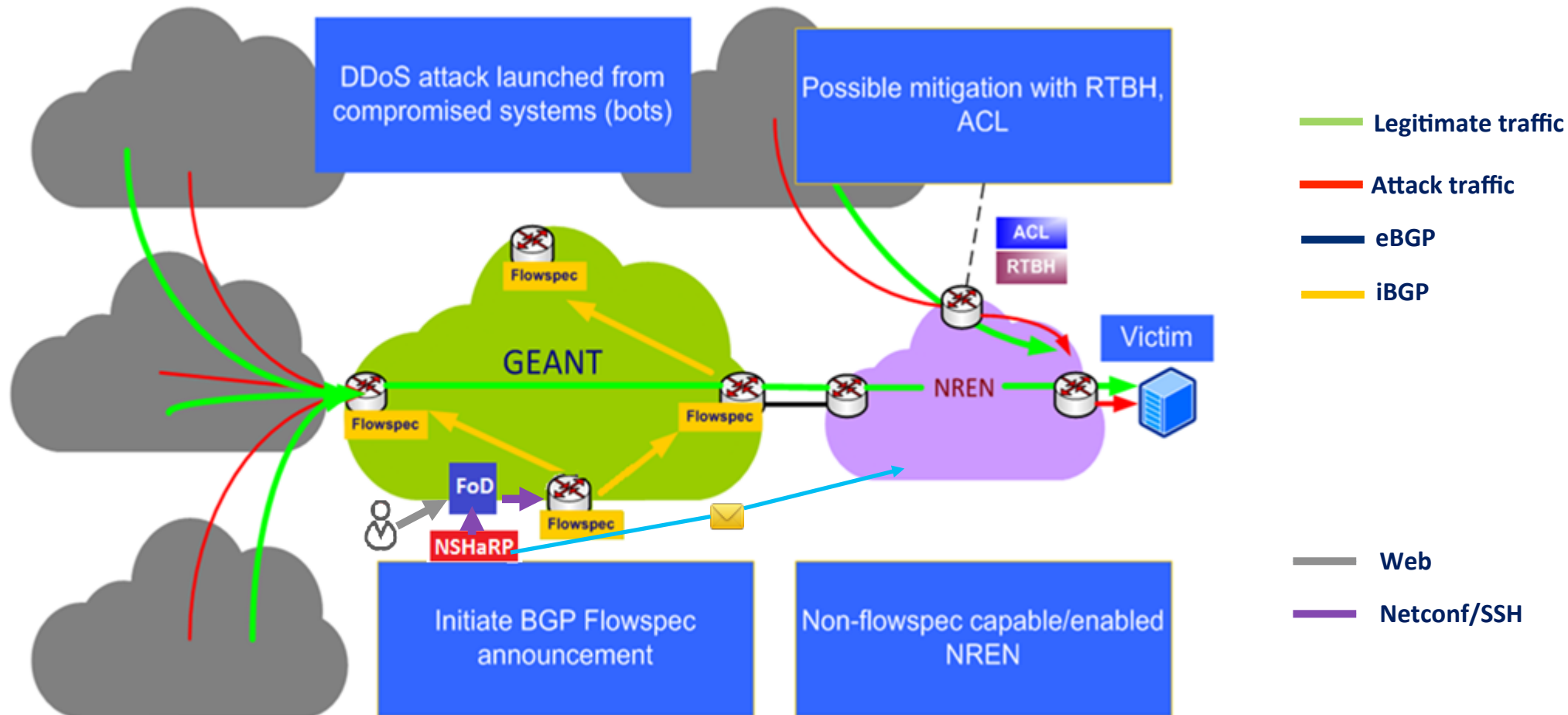


## Any issues?

---

- **BGP Flowspec**
  - eBGP flaps on 12.3R6.6 JunOS – currently running 13.2R4-S2 (but haven't tested eBGP)
- **FoD Application - RHEL**
  - Easier to install on Debian Wheezy
  - Some applications not natively supported – e.g gunicorn & celeryd

# I definitely like it!! But I want some more!!



Do **YOU** want to keep out the bad guys?







# GÉANT

**ASSOCIATION**

Networking • Services • People

## Thank you!

[Security@dante.net](mailto:Security@dante.net)

[Evangelos.Spatharas@dante.net](mailto:Evangelos.Spatharas@dante.net)