

Firewall on Demand

User Guide



February 2016

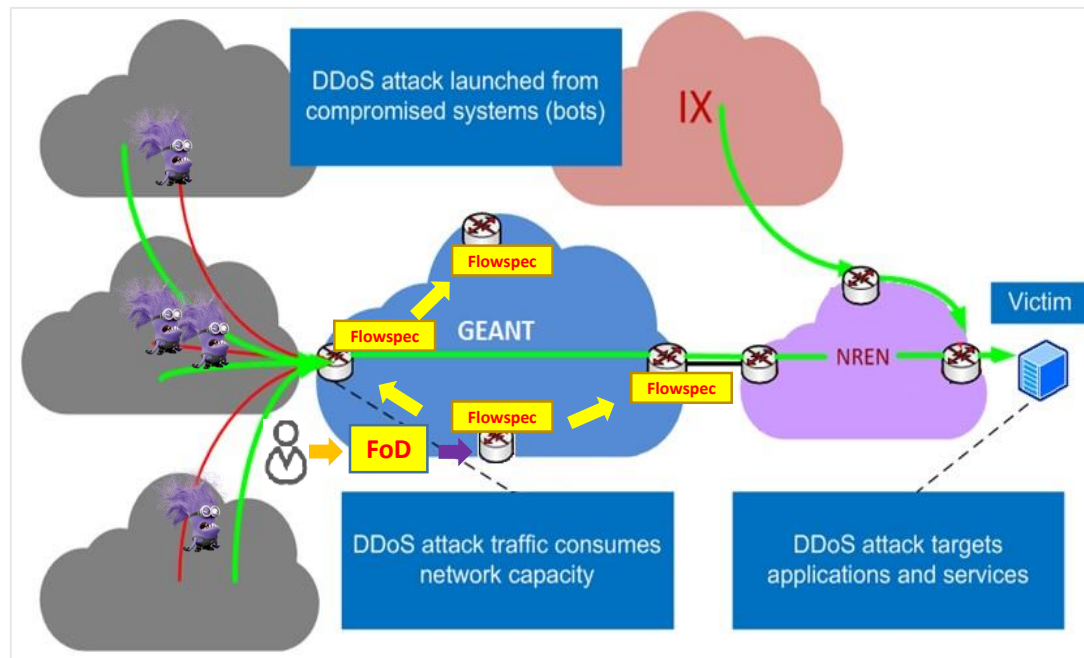
Contents

- Introduction
- FoD Capabilities
- FoD Requirements, Constraints and Limitations
- Eligibility and How to Subscribe
- How To Use

- Firewall on Demand (FoD) is a system which allows authorised users, via a web portal, to quickly create and disseminate firewall filters based on traffic flows to or from their designated address space
- FoD's key features are:
 - Precision – specific malicious flows can be targeted
 - Speed - Time to disseminate/withdraw firewall filters is sub 10 seconds
 - Convenience - NREN users can use web portal themselves, or make request by phone or e-mail.
 - Simplicity - The web portal uses intuitive, non-vendor specific GUI-based wizard to configure router firewall filters.
- FoD is powered by standards-based flowspec technology as specified in RFC 5575.

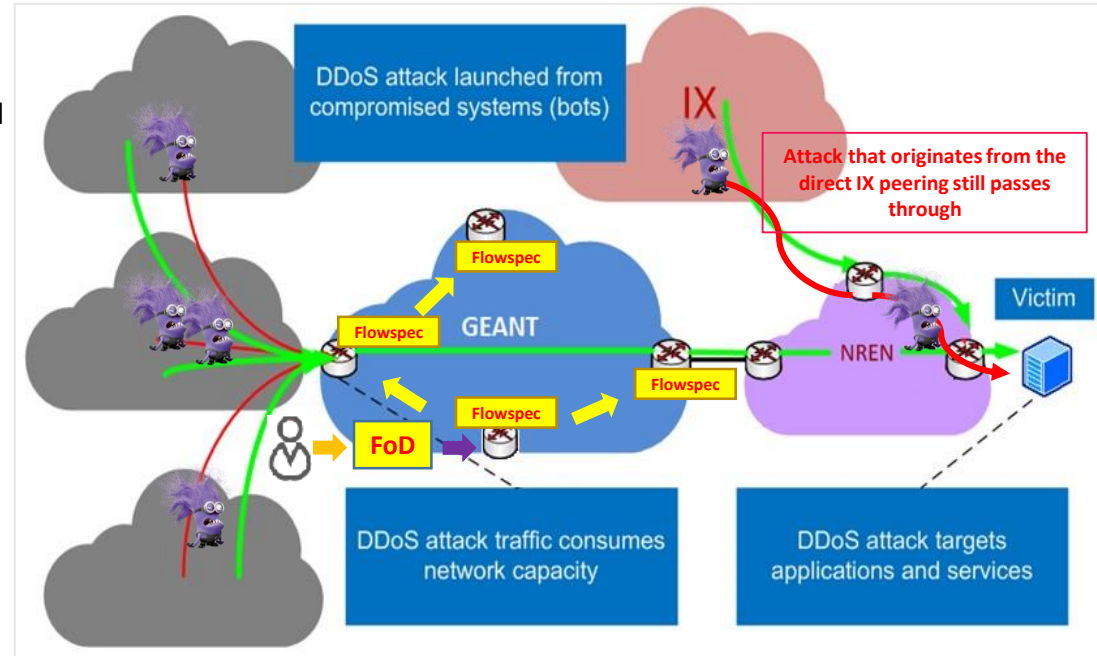
FoD Capabilities

- Propagate flowspec filters across GEANT backbone network
- Unlimited filters
- Have an e-mail sent to yourself or ticketing system for tracking after rule submission/edit/withdrawn
- Historical record – users can view all rules (active and de-active) created by themselves or their colleagues



Requirements, Constraints and Limitations

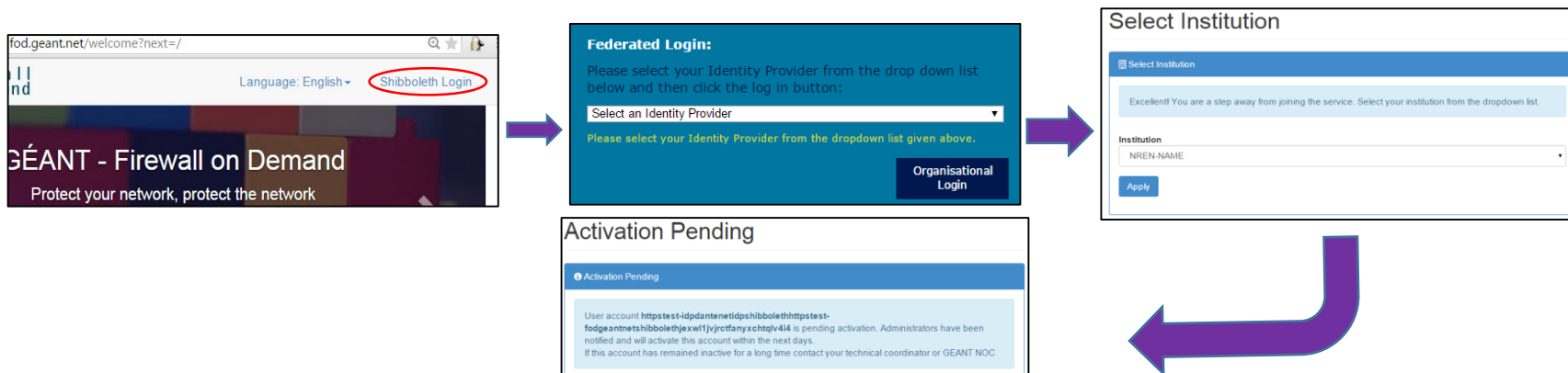
- Users can only create rules related to flows destined for their IP address space
- Only affects flows transiting GÉANT core routers
- IPv6 not currently supported
- Access to web portal limited to pre-specified users, accessing from a specific, pre-specified sub-net



Eligibility and How to Subscribe and Access

All GÉANT member NRENs may subscribe. The subscription process is as follows:

1. NREN APM fills out the FoD application form (MS Excel based) – NREN authorized users (by e-mail address); NOC subnet (for white-listing); NREN's AS number or AS-set.
2. NREN APM sends completed form to GÉANT security team (security@geant.org) and info is entered into FoD
3. Authorised NREN user, using host in NOC subnet, accesses <https://fod.geant.net> and clicks at the “Shibboleth Login” button on the top right. Login in using standard eduGAIN method
4. New user's account will be activated within 1 business day (assuming login details match info provided by APM)



FoD's Shibboleth module requires the release of the following attributes:

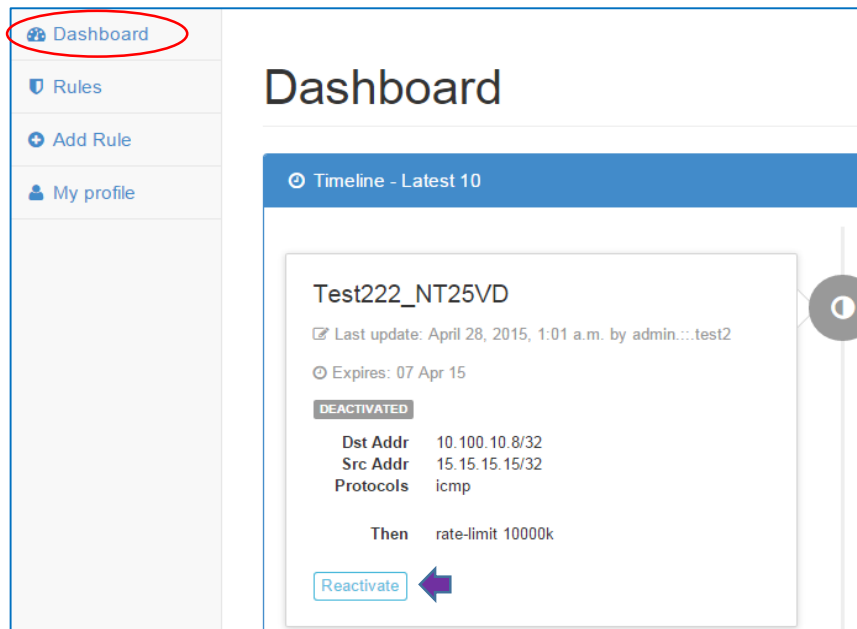
- givenName
- mail
- persistent-id
- principalName
- Surname (family name)
- uniqueID

New user's are notified by e-mail when their accounts are activated and at that point they are able to start using Firewall on Demand.

- Re-visit the <https://fod.geant.net> page and click on the “Shibboleth Login” button
- Once logged in standard users have access to 4 tabs:
 1. Dashboard
 2. Rules
 3. Add Rule
 4. My Profile

How to Use FoD – Dashboard page

Dashboard page displays the latest 10 rules that have been submitted for the user's Institution (NREN) along with their current status. Deactivated rules can be re-activated and vice versa.



The screenshot shows the FoD Dashboard interface. On the left is a sidebar with navigation links: 'Dashboard' (highlighted with a red circle), 'Rules', 'Add Rule', and 'My profile'. The main content area is titled 'Dashboard' and features a 'Timeline - Latest 10' section. A rule card for 'Test222_NT25VD' is displayed, showing its last update, expiration date, and status as 'DEACTIVATED'. The rule details include Dst Addr (10.100.10.8/32), Src Addr (15.15.15.15/32), Protocols (icmp), and an action 'Then rate-limit 10000k'. A 'Reactivate' button is visible at the bottom of the rule card, with a blue arrow pointing to it.

Dashboard

Timeline - Latest 10

Test222_NT25VD

Last update: April 28, 2015, 1:01 a.m. by admin...test2

Expires: 07 Apr 15

DEACTIVATED

Dst Addr 10.100.10.8/32

Src Addr 15.15.15.15/32

Protocols icmp

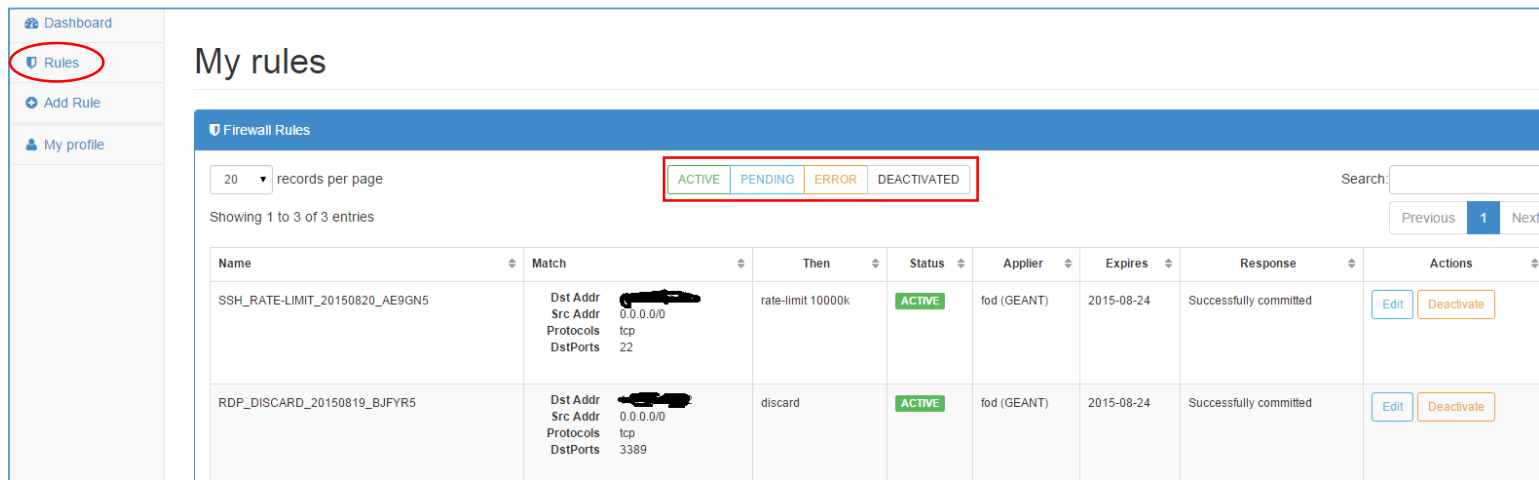
Then rate-limit 10000k

Reactivate

How to Use FoD – Rules Page

The Rules page displays ALL (not just the latest 10) rules that have been submitted for the user's Institution, sorted by status. From here, any rule can be reactivated, deactivated or edited.

A search box is available to look for particular rules



Dashboard

Rules

Add Rule

My profile

My rules

Firewall Rules

20 records per page

ACTIVE PENDING ERROR DEACTIVATED

Search:

Previous 1 Next

Name	Match	Then	Status	Applier	Expires	Response	Actions
SSH_RATE-LIMIT_20150820_AE9GN5	Dst Addr Src Addr Protocols DstPorts 0.0.0.0/0 tcp 22	rate-limit 10000k	ACTIVE	fod (GEANT)	2015-08-24	Successfully committed	Edit Deactivate
RDP_DISCARD_20150819_BJFYR5	Dst Addr Src Addr Protocols DstPorts 0.0.0.0/0 tcp 3389	discard	ACTIVE	fod (GEANT)	2015-08-24	Successfully committed	Edit Deactivate

How to Use FoD – Add Rule Page

New rules have four mandatory attributes, which are indicated by field labels in bold:

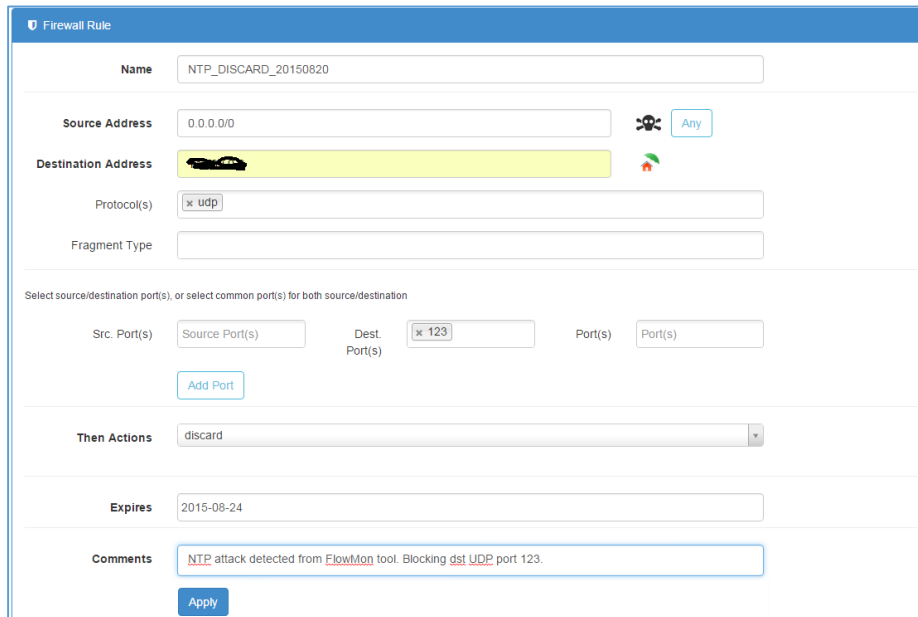
- Name
- Source Address
- Destination Address - ***must belong to NREN***
- Then Actions

By default, a filter expires after 7 days from its submission, but you can specify any time between 1 – 10 days (will be more flexible in future)

It is strongly recommended that the rule's name uses the following format:

<TYPE_OF_ATTACK>_<ACTION>_<DATE>[_INCREMENT]

Where 'increment' is a suffix of '_1', '_2' and is used if more than one rule of the same type is created on a given day.



Firewall Rule

Name: NTP_DISCARD_20150820

Source Address: 0.0.0.0/0

Destination Address: [Redacted]

Protocol(s): [x] udp

Fragment Type:

Select source/destination port(s), or select common port(s) for both source/destination

Src. Port(s): Source Port(s) Dest. Port(s): [x] 123 Port(s): Port(s)

Add Port

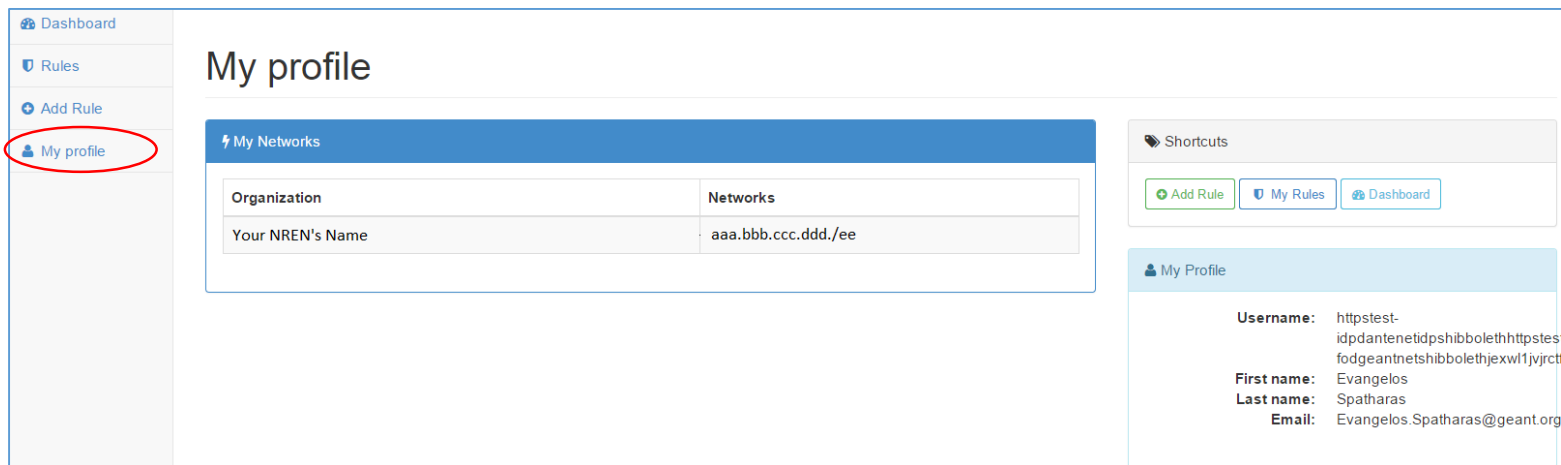
Then Actions: discard

Expires: 2015-08-24

Comments: NTP attack detected from FlowMon tool. Blocking dst UDP port 123.

Apply

My profile page displays information that has to do with the user's subscription such as their administrative network and name, your username and e-mail.



My profile

My Networks

Organization	Networks
Your NREN's Name	aaa.bbb.ccc.ddd./ee

Shortcuts

[Add Rule](#) [My Rules](#) [Dashboard](#)

My Profile

Username: httpstest-idpdantenetdpshibbolethhttpstesfodgeantnetshibbolethjexwl1jvrct

First name: Evangelos

Last name: Spatharas

Email: Evangelos.Spatharas@geant.org

For all issues or queries related to FoD, please contact GÉANT Infrastructure & Security team at security@geant.org