Firewall on Demand

User Guide

February 2016

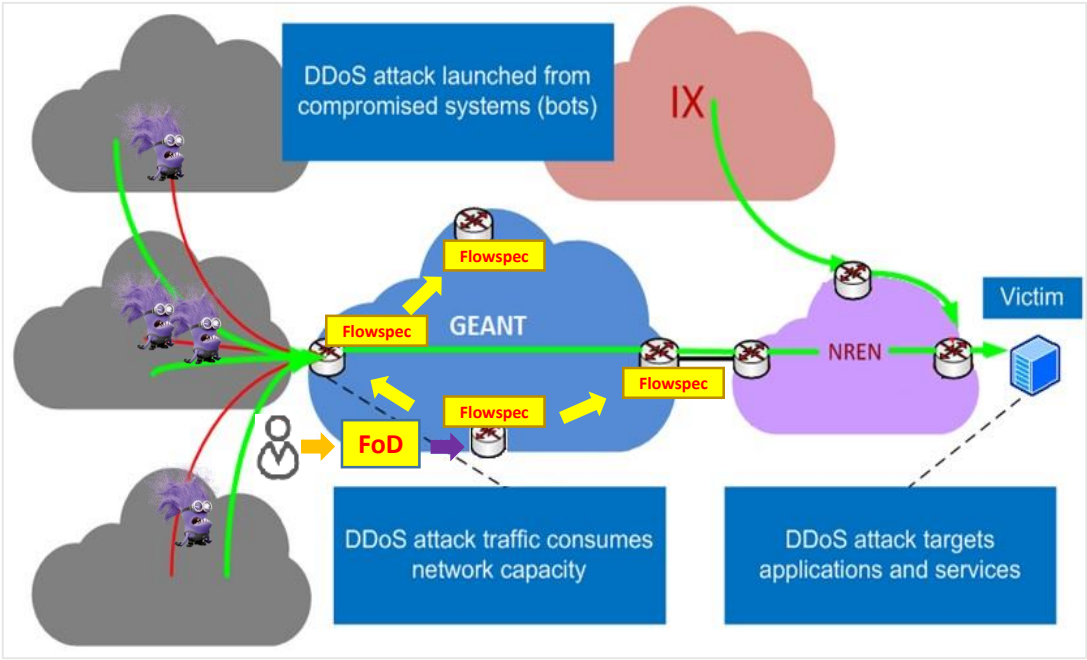
Contents

Firewall on Demand - Introduction

- 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.

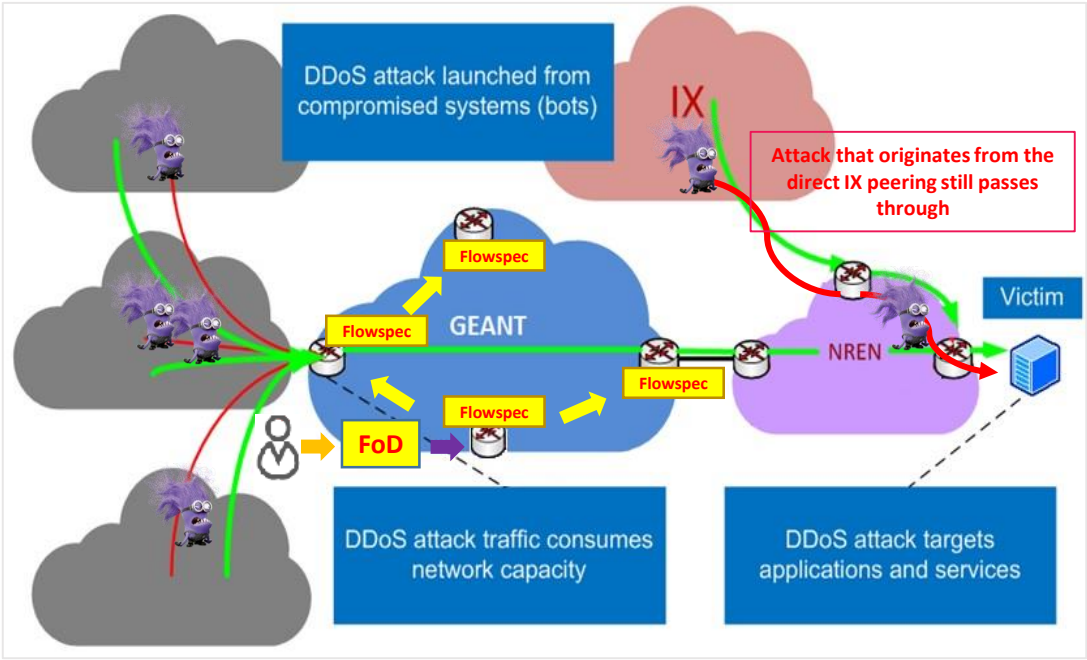
FoD Capabilities

- 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- Have an e-mail sent to yourself or ticketing system for tracking after rule submission/edit/withdrawn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

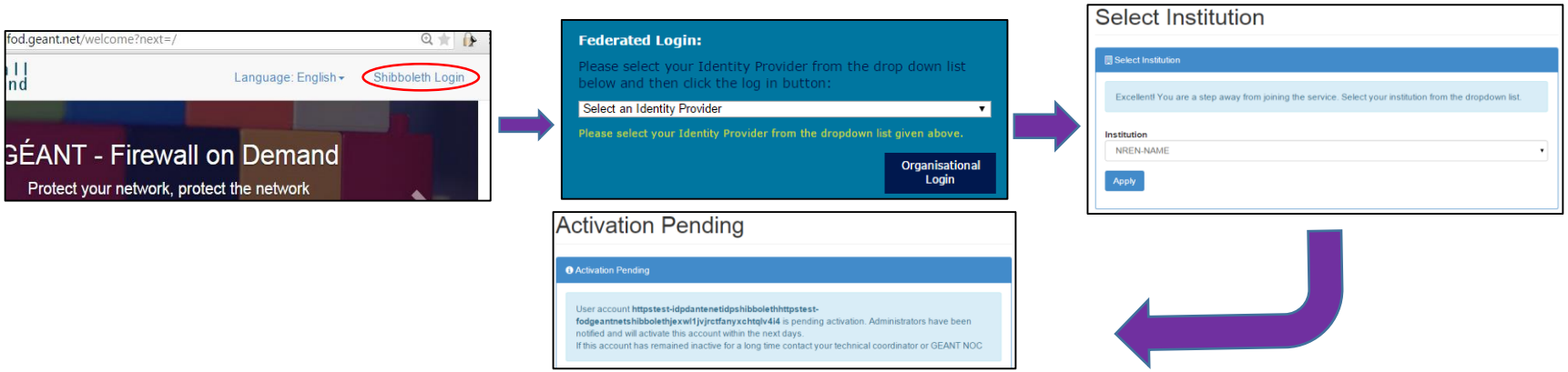
- Users can only create rules related to flows destined for their IP address space
- Only affects flows transiting GÉANT core routers
- IPv6 not currently supported
- Access to web portal limited to pre-specified users, accessing from a specific, pre-specified sub-net



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)



Shibboleth Attributes

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

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

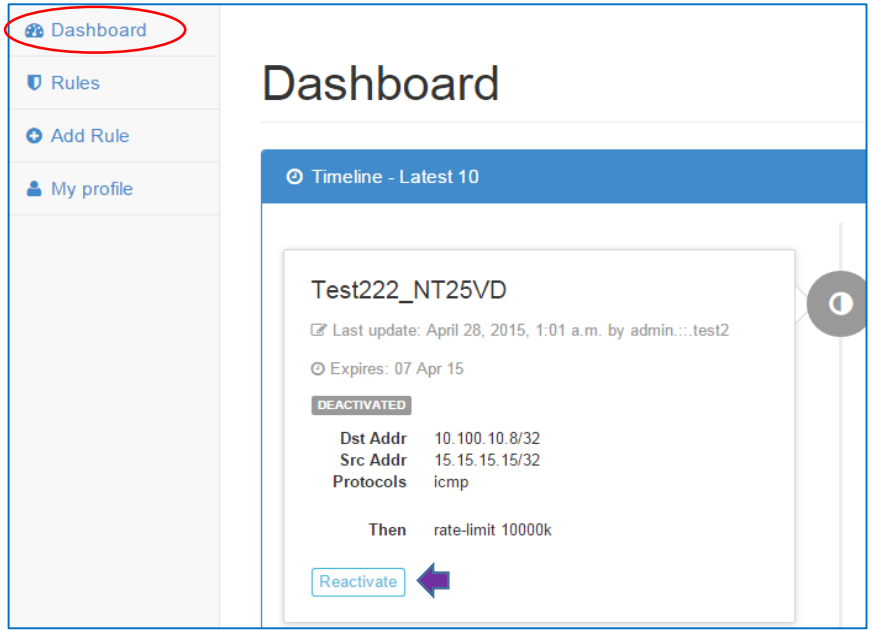
How to Use FoD

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

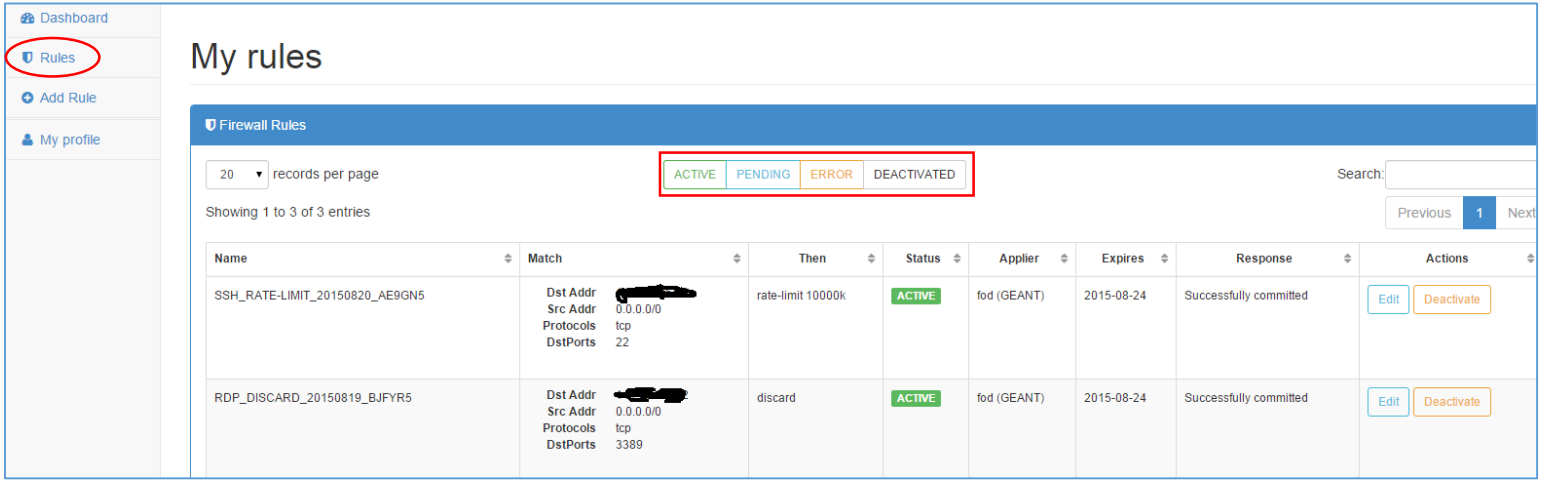
Dashboard page displays the latest 10 rules that have been submitted for the user's Institution (NREN) along with their current status. Deactivated rules can be re-activated and vice versa.



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



How to Use FoD – Add Rule Page

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

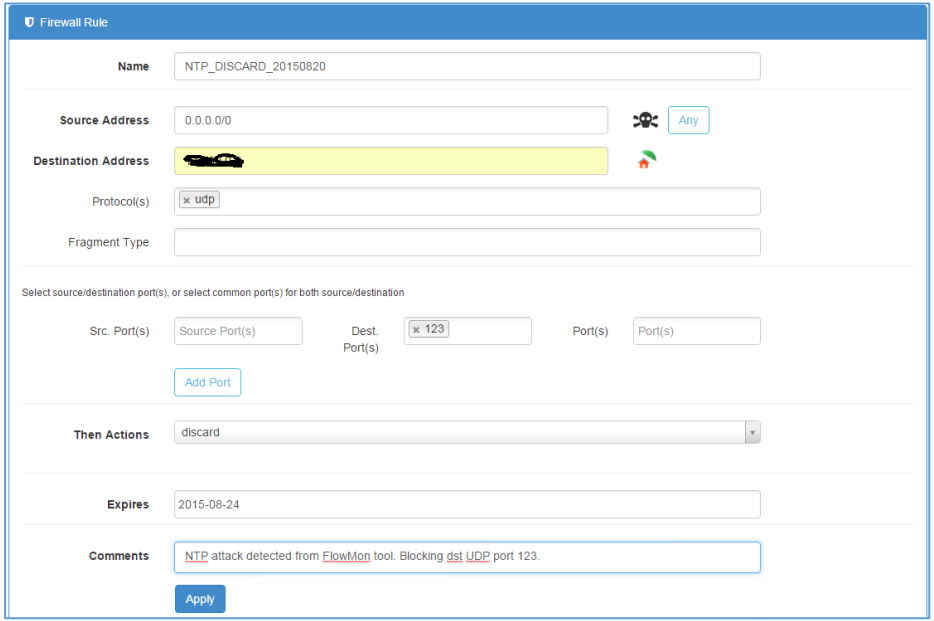
- Name
- Source Address
- Destination Address - ***must belong to NREN***
- Then Actions

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:

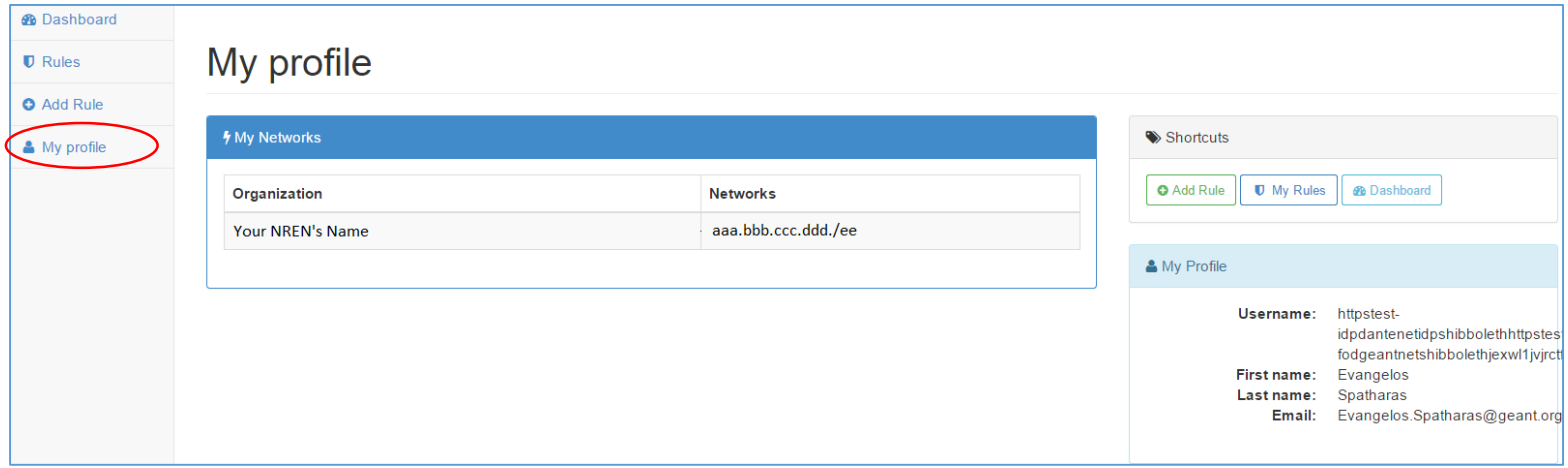
<TYPE_OF_ATTACK>_<ACTION>_<DATE>[_INCREMENT]

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



How to Use FoD – My Profile Page

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.



How to Contact us

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