Firewall on Demand Training

Introduction

GEANT Information & Infrastructure Security Team

September 2016
Contents

• Introduction
• FoD Capabilities
• FoD Requirements, Constraints and Limitations
• Eligibility and How to Subscribe
• How To Use
Firewall on Demand - Introduction

• Firewall on Demand, abbreviated as FoD, is an application with a WEB front which allows subscribed users to disseminate firewall filters easily without any hassle.

• 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.
  • No interaction* (e-mail, phone call) with GEANT NOC is required. NREN user can add/remove filters at its own discretion.
  • No special knowledge of router-language is required. The WEB based app offers a very friendly scheme for applying the filter.

• The magic of FoD is powered on by the cutting edge flowspec technology as described by the RFC 5575.

*NOC/CERT users can still contact GEANT CERT using the traditional methods to request blocking
FoD Capabilities

- Propagate flowspec filters across GEANT network
- Filters CAN have DST address from YOUR administrative IP space
- Have an e-mail sent to yourself or ticketing system for tracking after rule submission/edit/withdrawn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-activated) created by themselves or their colleagues
Requirements, Constraints and Limitations

- Only affects flows transiting GÉANT core routers
- IPv6 is not currently supported
- Propagate a filter with a DST subnet bigger than /29
- Access FoD platform from an IP space other than your NOC’s/GEANT network’s space
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 Partner and Relations team (partner-relations@geant.net) and info is entered into FoD.
4. New user’s account will be activated within 1 business day or less (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
How to Use FoD

After your account is activated for which you’ll be notified by e-mail, you are ready to start Firewall-ing on Demand. The process is as simple as follows:

• Re-visit the https://prod-fod.geant.net page and click on the “Shibboleth Login” button

• After supplying with your credentials you’ll have access to 5 main tabs:
  1. Dashboard
  2. Rules
  3. Add Rule
  4. My Profile
  5. Admin
How to Use FoD - Dashboard

Dashboard page displays the latest 10 rules that have been submitted for your Institution along with their current status. Deactivated ones can be re-activated and vice versa.
How to Use FoD - Rules

Rules page displays ALL (not just the latest 10) the rules that have been submitted for your Institution, sorted by status. From here, you can reactivate or deactivate rules, or even edit them.

What is more, one can use the search box to look for particular rules and process them further.
Add rule page is the place where you navigate when you first see an attack. To add a rule requires to populate all the necessary fields which are the following:

- 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:

**Note:** It is recommended that the rule’s name is of the following format:

<NREN/Peering/IC>_TYPE_OF_ATTACK_<ACTION>_<DATE>

This will aid you in the future when searching for a rule.
How to Use FoD – My Profile

My profile page displays information that has to do with your subscription such as your administrative networks and name, your username and e-mail.
In case you have any issues or queries in relation to FoD, please contact GÉANT Infrastructure & Security team at security@geant.org