24-01-2020

Milestone M8.4
FoD Future Development Requirements Analysis

Milestone M8.4

Contractual Date:	31-01-2020
Actual Date:	24-01-2020
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 3
Nature of Milestone:	O (Other)
Dissemination Level:	PU (Public)
Lead Partner:	DFN/LRZ
Document ID:	GN43-20-1422AD
Authors:	Evangelos Spatharas (GEANT Assoc) David Schmitz (DFN/LRZ)

© GÉANT Association on behalf of the GN4-3 project.
The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract
This document presents the results of the FoD Future Development Requirements Aanalysis, covering the development, testing, and support of Firewall on Demand (FoD).

Table of Contents

1 Introduction

This document presents the results of GN4-3 WP8 T3 milestone "FoD future development requirements analysis", covering the development, testing, and (service and software) support of Firewall on Demand (FoD).

This is intended to be a working document that will continue to be updated during the whole course of GN4-3 to align it to users' requirements.

This document is structured as follows:

- Section 2.1 provides an overall description of FoD.
- Sections 2.2 and 2.3 respectively cover FoD changes in GN4-2 and in GN4-3 to date to provide a starting basis.
- Section 2.4 identifies and compiles all potential open issues or ideas from previous project phases.
- Section 2.5 discusses the general FoD development areas from the GN4-3 Description of Work and what they might involve in terms of FoD development/testing and support.
- Based on the potential areas of improvement identified, a user study was conducted and its results analysed. This is covered in Sections 3.1 and 3.2.

Future versions of this document will be updated to further reflect and align with iterative current user requirement analysis steps, either selecting from or adding to the pool of open issues.

2 FoD Development Analysis

2.1 What is FoD

Firewall on Demand (FoD) is a BGP-FlowSpec-based [FlowSpec] DDoS mitigation solution which was developed in earlier phases of the GÉANT project [GnFoD] and is currently provided in the GÉANT core network as a productive service to allow users (NREN NOC administrators) to administer BGP FlowSpec rules via a web interface. This allows them to filter normally routed GÉANT IP traffic based on the administered BGP FlowSpec [FlowSpec] [Redirect] rules.

In addition to the production service for GÉANT core network's traffic, FoD server software is free to be installed and run by anyone, specifically targeted at other NREN NOCs.

2.2 FoD Development Before GN4-3

In the previous phase of the GÉANT project, GN4-2, several functionalities improving user experience were developed, tested and eventually released in FoD v1.5 which has been in production since autumn 2018:

- An explicit specification of UDP/TCP port ranges is now available overcoming the need to list every single port within an intended port range in the specification.
- Statistics graphs per active rule provide a feedback about the effectiveness of ongoing DDoS mitigation (packets/bytes dropped per rule over time) and can give indications when an active mitigation rule might be decommissioned after the targeted DDoS attack actually stopped.
- A rule control REST API allows the automated querying, creation, change and deletion of rules.

In addition to the functionalities added for the production FoD v1.5, development and testing was performed for the semi-automated proposal of mitigation rules based on DDoS attack events during GN4-2. This resulted in the development of a prototype for a DDoS detection and mitigation system based on FoD. To this end, the rule control REST API added earlier was utilised in combination with a Warden server [Warden] and RepShield [RepShield] server developed by CESNET. Warden server was selected as a generic security alarm/event hub using a lightweight JSON-based event format IDEA [Idea] for security alert sharing. It was specifically used here to receive security alarms converted from GÉANT's Network Security Handling and Response Process (NSHaRP) [NSHaRP] messages about DDoS attacks detected in GÉANT's core network traffic,

In turn, any alarms for DDoS attacks received by the Warden server are forwarded to a new component, the Firewall Rule Updater (FRU), whose task it is to create BGP FlowSpec mitigation rules in FoD, via FoD's rule control REST API, based on the attack information in the forwarded alarms.

These rules are created as proposals for the administrators of the attacked network in an inactive state, allowing the administrators to check and edit the rules as needed. FRU currently proposes multiple mitigation rules which represent different mitigation strategies for a single detected attack. Some of these strategies require additional rating information, known as a reputation score, about attacker IP addresses, which is calculated and maintained by the RepShield server. For this purpose, the RepShield server is forwarded any alarm received by the Warden server, including DDoS attack-related ones, and correlates them with additional information from other available security-related information sources, e.g. specific blacklists.

The FoD used for this semi-automated mitigation proposal needed several enhancements of the FoD's rule control REST API developed for FoD v1.5, e.g. an extended concept allowing a single FoD mitigation rule to cover multiple attacker IP address prefixes, resulting in multiple BGP FlowSpec rules. Currently these enhancements are still experimental, therefore, they were not included in production version 1.5. Instead, they will be part of version 1.6.

The final user testing of the prototype for a DDoS detection and mitigation system based on FoD v1.6 identified some recommendations for improvements, especially regarding usability and better user control of rule proposals.

FoD v1.5 and the testing are covered inDeliverable D8.2 *Firewall-on-Demand Progress Report* [D8.2] and the Firewall-On-Demand 1.5 Pilot Results from May 2018 respectively, while the DDoS detection and mitigation system using FoD v1.6 is covered in Deliverable D8.3 *Distributed Denial of Service Mitigation v1.0 Pilot* [D8.3] and Deliverable D8.12 *Distributed Denial of Service Mitigation v1.0 Pilot Follow-up* [D8.12].

2.3 FoD Development in GN4-3 To Date

After the production release of FoD v1.5 some issues were experienced by users:

- Statistic graphs were not created for mitigation rules which used IP fragmentation filter options. This is a direct limitation in the code developed for v1.5.
- eduGAIN login errors are cumbersome and do not really indicate the actual error. This is a pre-existing issue not specific to v1.5. Error messages are hardcoded into FoD's code and do not take into account the possibility of flexibly and generically changing eduGAIN Shibboleth authentication attributes in FoD's configuration settings.

Both issues had only been partially investigated and therefore not fully fixed and tested at the end of GN4-2.

For this reason, the first months of GN4-3 were devoted to addressing both issues. An update of FoD v1.5 fixing both issues is now being tested by the FoD service operators and it is expected that it will soon be released for the production service.

Beyond the support for the GÉANT FoD service, installations support for FoD in other NRENs was always somewhat limited due to insufficient time to properly reproduce errors reported by other users who were testing the FoD installation within their own environments. To overcome this, work on docker-based containers for FoD was started. This will provide users of the software with a fully working reference container-based installation of FoD which they can either use to compare and fix their own installation trials, or even directly as a container-based FoD instance. In addition, different, adapted FoD containers for the various operating environments can be developed to reproduce and understand errors encountered by users of the software.

The developers also identified some issues regarding the versions of the software stack used:

- Update / test FoD to support newer Python dependencies.
- Upgrade FoD to support Python 3, as Python 2 is deprecated and only supported until end of 2019.

Consequently, work has been undertaken to transition FoD code to Python 3 along with replacing all Python dependencies with Python 3. This work is not fully finished but the Python 3-based FoD web UI is working fully so far. REST API is only partially functional and Shibboleth user registration is missing.

2.4 Open Issues and Future Development Ideas from Previous Project Phases

This section summarises all known open development issues, requests or ideas for improvement or introduction of new functions in FoD from previous project phases that were put forward by the developers/operators (internally) or users of the service or the software (externally).

This collection will form a part of the initial basis for future user-aligned requirements analyses to determine the work to be done and priorities regarding the development, testing and support of FoD in GN4-3.

Before the GN4-2 phase, a number of open development issues, requests or ideas were collected by the GÉANT FoD service operator. Those which are still open are summarised here, grouped into the following broad categories:

- FoD user functionality (in web UI):
  - IPv6 support: support for propagation on IPv6 BGP FlowSpec depends on the routers used. Current GÉANT core routers do not support it, due to an old Juniper OS version. In GN4-2, FoD was analysed and considered to be ready for IPv6. Tests with FoD and a test router which support IPv6 propagation may be performed to confirm this.
  - Full support of all RFC-5575 (FlowSpec protocol) fields. (Includes DSCP marking redirect to other VRF table etc.)
  - Online help prompt showing expected rule format in the rule name field: e.g. ‘Split the 'Name' field into 4 columns, perhaps auto-created based on some other fields, and only ask the user for the attack type, helping users to follow the rule format.

- Inflexible rate limiting (currently only 3 fixed choices for bandwidths (1k, 10k, 100k) are available).
- Ability to install a permanent rule.
- Ability to install a rule which will become active in the near future, e.g. to be used in maintenance windows.
- Visibility of rules affecting a particular peer between users.

- FoD user functionality (download/export functions):
  - Ability to download reports to local user's machine from the UI: this already partially addressed by new rule-control REST API, but not in an easy way (e.g., CSV or PDF; no easy filtering is possible; not yet integrated with mitigation statistics).
  - GUI to allow users to download a file containing rules profile configuration of FoD: this is partially addressed by the rule control REST API, but not in a user-friendly manner.

- FoD admin functionality (of an installed FoD instance):
  - Admin interface and internal configuration: Integrate AS numbers as part of a user profile instead of the current IP prefixes. Populate and update the IP prefixes of an NREN automatically by using the AS numbers provided, ensuring that the administrative space of an NREN/peering is always up to date. Currently the FoD admin has to do this manually.
  - Action log per individual FoD user's actions, for Accountability and incident (misuse & accidental use of FoD) detection and handling – either in a log file on the server (simple form) or log accessible in admin web UI (enhanced form).
  - Display the exact time the rule was applied/expired in “My Rules” pages and log files: e.g. to be used for auditing related to the time taken until reaction against the attack.
  - Automatic FoD rules profile configuration backup and restore functionality with GUI to control DB backups.

- FoD operation security (in general):
  - No more than 20 active rules for any given peer: eliminates e.g. the possibility of a compromised account for DoSing its own IP space with FlowSpec rules.
  - Website session expiry after 20 minutes inactivity for security reasons.

- FoD low-level internal communication to mitigation hardware (currently only BGP FlowSpec-enabled routers are supported)
  - Public key authentication between FoD and FlowSpec-enabled router, instead of currently using password over SSH.
  - FoD ncclient module (SSH NetConf access) to use 'configure private' instead of 'configure exclusive' on Juniper CLI: prevention of conflict with other services using a GÉANT resource.
  - Possible to place FlowSpec rules into more than one routing table.

- FoD installation functionality/support:
  - Ability to customise configuration settings of FoD from the admin web UI, e.g. upload company logo, icon, choose language etc. This would make installation easier and so increase the scope of the users.

- FoD software upgrade GUI with notifications and ability to upgrade local instance of software.

During GN4-2 the following issues and improvement ideas were identified by developers, operators and testers:

- Improve Graph navigation in general, e.g. use a more flexible graphing JavaScript library, which supports zooming in time.
- Improve accuracy of the relative-value graphs.
- Rule Names: allow characters beyond letters, numbers and underscore in rule names.
- Improve the user's understanding of some parts of the UI by providing short explanations, examples and hints, e.g. regarding missing statistics for never-activated rules, explanation of what exactly a drop limit of 100k means (bytes/packets?), etc.
- Support of multi-factor authentication, e.g. via Google Authenticator.
- v1.6 DDoS detection prototype (ideas from developers and testers):
  - Allow the display of rules in groups in the UI, e.g. group of all rules created by FRU for a particular event.
  - Introduce general tag mechanism for rules to allow flexible grouping, editable by the user.
  - More clearly indicate a rule proposed by FRU as such in the UI, allow users to delete (or ignore in the UI) the rule explicitly if it is never activated by them.
  - Add user settings to the UI for configuring the rules proposal, e.g., allow disabling it completely.
  - Add a user setting for configuring an interval to auto-deleted unused proposed rules.
  - Auto-delete proposed rules that the user has not used after a specified interval, e.g., default 1 week.
  - Improve rule comment and info mail to more clearly indicate that it was proposed automatically by FRU.
  - In-rule Add/Edit form: add notes that rate-limit applied to multiple destination IP prefixes will apply separately for each prefix.

During GN4-2 the following ideas were raised by users and the general audience at various project meetings:

- Automated feedback loops, e.g. utilised when a rule is no longer needed as indicated by the mitigation statistics.
- Support for automated, dynamic change of rules over time, based on definition of complex attack types.
- In UI better filtering/searching to provide better overview and handling of many rules.
- Consider conflicting rules: e.g. overlapping IP prefixes of users in configuration, as well as rules where attacker prefixes overlap with the IP prefix of another user.
- Interconnection of different FoD instances (GÉANT<⇒NREN<⇒institution)

During GN4-2 the following new recommendations/ideas were raised by an installation tester:

- Make the REST API easier to handle (complicated recursive REST object dependencies, certain numbers, e.g., IP protocols such as UDP/TCP, are defined as potentially varying values in DB, which is cumbersome to use and could cause mismatches).
- Switch to using JSON web token-like standards.

2.5 Development Ideas and Possible Directions in GN4-3

Any of the issues and ideas listed in the previous section may be addressed in GN4-3, where they are found to be appropriate, useful and necessary based on any future user-based requirement analysis that is carried out.

However, the Description of Work for the current GN4-3 project phase outlined four specific areas which are expected to attract the most attention and on which the main focus is likely to be in terms of development/testing and support for FoD in the project phase. These areas and what they involve in terms of potential investment of effort are discussed below.

These four general areas are:

- Area 1: Firewall on Demand as multi-domain interface to allow integration into the coordinated DDoS mitigation across multiple domains (GÉANT, NRENs, institutions).
- Area 2: Delivery of attack and monitoring data to improve analysis by CERTs and SOCs.
- Area 3: Generalised multi-domain Firewall on Demand interface supporting FlowSpec and, if necessary, additional protocols.
- Area 4: Web application firewall functions.

A new key aspect for FoD development/support in GN4-3 is the cooperation with WP8 T3.3, which is responsible for the development and support of a central, integrated DDoS detection and mitigation solution that will rely strongly on the GÉANT FoD service as one type of mitigation. This cooperation is mainly related to Area 1, but more broadly also to the other areas. Furthermore, to contribute to a fully reliable DDoS detection and mitigation workflow, including the current mitigation in the BGP FlowSpec-enabled routers, the testing and verification of FoD functions and interfaces has to be extended and made ready to be performed on a regular, repeatable, and ideally automated basis.

The interplay of rules submitted from the central DDoS mitigation solution via FoD to the routers and the current filtering/rate-limiting of actually targeted attack traffic has to be made verifiable, automatable and repeatable. This is at least required in the case of any updates of any service or component taking part in the central DDoS detection and mitigation process, e.g. FoD, the routers, the detection systems, etc. Previously, such tests were run only on a manual basis, not covering any corner cases of combinations for filter options. A more regression-like testing manner which can be repeated on a regular basis would be a greatly appreciated improvement.

More generally, the following potential activities can be derived for each of the four areas:

Area 1

- Enhance the existing high-level DDoS detection rule exchange/sharing (i.e. FoD rule control REST API) in line with user requirements.
- For this purpose, liaise with users (NREN NOCs), e.g. provide concrete implementation/code examples for particular tools (e.g., NfSen, Cacti, Nagios) currently used by the users for DDoS detection.
- Liaise with WP8 T3.3 (and GN Security) regarding the requirements, testing, enhancing and regular use of the FoD DDoS mitigation rule API by this task.
- Liaise with GN Security (and WP8 T3.3): investigate how FoD development can help to test, verify and ensure (initially and regularly) a stable FoD mitigation service to be used by WP8 T3.3.
- On a lower (technical) level, check whether or how far to share BGP FlowSpec rules via eBGP with NRENs. Liaise with FoD operators and FoD users (NREN NOCs).

Area 2

- Design means to exchange and share mitigation statistics with users.
- Design means to exchange attack data (events of actual attacks, means to verify/simulate attacks) between users of the FoD user community.
- For this purpose, liaise with users, generally NREN NOCs, using FoD, WP8 T3.3, WP8 T3.1, and possibly WP8T3.2.

Area 3

- Generalise DDoS detection/mitigation low-level/technical interface (beyond BGP FlowSpec) and extend internal rule design accordingly.
- An example of another mitigation technology is the recently acquired A10 DDoS mitigation box. This will be run in future by the GÉANT Security team. Therefore, liaise with GN Security (and future users) to see how to use FoD to enable a multi-tenant access to the mitigation functions (control; status; statistics - via webUI and REST API) of this service for users in a way which is compatible and seamlessly integrated with the current BGP-FlowSpec-based FoD service.
- Potentially, assess SDN/OpenFlow solutions for DDoS mitigation. This requires too much manpower, but could possibly be done in cooperation with WP6 T1/T2, at least to carry out some investigations (e.g., market analysis, checking of upcoming IETF standards as, e.g., DOTS, I2NSF) regarding this.

Area 4

- Investigate options how web application firewall functionality (as kind of Layer-7 DDoS mitigation) can be provided to FoD users (=NREN NoCs).
- Liaise with users and WP8 T3.3 regarding this.
- Liaise with GÉANT Security who will operate the A10 DDoS mitigation device which might be able to already provide such mitigation functions.

- Extend internal FoD rule design to comprise also such Layer-7 DDoS mitigation rules.
- Provide low-level (technical) means to perform web mitigation functions, e.g. via the A10 box. Get status and statistics during mitigation.
- Extend the rule control API and mitigation statistics exchange means (see Area 2) accordingly, in cooperation with users.

Beyond the four areas from the Description of Work and the relative conclusions drawn, some further open issues and ideas have arisen since the beginning of GN4-3:

- A new idea for a novel user functions identified since the start of GN4-3 is to
- effectively handle TCP syn attacks (a type of non-volumetric DDoS attack).
- The work to transition FoD code from Python 2 to Python 3 along with replacing all Python dependencies with Python 3 equivalents has been started and is in quite an advanced stage.
- Beyond anything mentioned, it is expected that new future ideas can be found and evaluated by users. For this purpose and the evaluation of the existing open issues and ideas listed above, a user community around DDoS should be established. This community could be updated regularly regarding all FoD development, testing and support, using, e.g., periodic meetings, VCs, presentations, newsletters, the wiki (e.g. for enhancement requests), and/or questionnaires. Thus, a user-aligned, prioritised list of requirements can initially be established, and then be regularly updated during the future course of the project.

3 User Study for Prioritisation of Requirements

3.1 User Interviews

In order to take into account the real needs of users, a user study was performed. This consisted of individual interviews with selected FoD service key users. Prior to the interviews, a list of questions was compiled which covered the main aspects of all the potential enhancements introduced in the previous sections. This list was sent to the interviewees beforehand.

Questions and answers

The questions are numbered Q1-Q10 and corresponding answers A1-A10 with the addition of a)-d) to differentiate between the answers of the various NRENs interviewed.

Q1) We are planning to make FoD the one-stop for mitigation, supporting FlowSpec, RTBH and scrubbing centre in the future. What is your opinion?

A1-a) Excellent. Would be willing to pay 20-50K per year for a good service. Cannot pay half million to commercial entities for mitigation as we are an academic ISP.

A1-b) Sounds like a good idea.

A1-c) Yes that would be good!

A1-d) As long as we don't lose access to that single point, yes it makes sense. Good idea. Avoid single point of failure.

Q2) What is your opinion about a multi-domain FoD where FlowSpec is propagated from an NREN to GÉANT and from GÉANT to all other NRENs?

A2-a) Not interested because FlowSpec is not used within in our NREN.

A2-b) Good idea.

A2-c) We need it. Because our NREN has a peering with NORDUnet and GÉANT.

A2-d) Most of the attacks are not between NRENs. Seems interesting if it can be an optional feature. We don't use FlowSpec.

Q3) Would your NREN be interested in testing and running a local instance of FoD using WP8 T3.4's docker image? Yes/No

A3-a) We don't need it. Access to GÉANT FoD is what we need. What is provided is good enough.

A3-b) Yes, but need to first install docker infrastructure.

A3-c) Yes, interested in testing.

A3-d) No because we don't have FlowSpec.

Q4) Do you find the REST API in general useful? Can you make some improvement recommendations?

A4-a) Not something that we really use. We use it once a month. Not really a need for REST API.

A4-b) Haven't had chance to test the REST API. No recommendations.

A4-c) We need a set of examples on how to make good use of it. Also, being able to get statistics.

A4-d) In the future we will investigate. An option for the future.

Q5) Would you recognize any value if FoD was able to provide for web app firewall functions?

A5-a) Don't see currently a need for that.

A5-b) At the moment don't see, we can discuss this in interview.

A5-c) Not very interesting to us.

A5-d) Idea: Reblays technologies from Israel. It would be interesting as commercial vendors won't be needed. Only limited use cases though.

Q6) Do you see attacks against IPv6 targets?

A6-a) It will be important, but not in the near future. We don't even know if there are attacks on the IPv6.

A6-b) Don't know, as I haven't noticed. Would like to have.

A6-c) No need for us, only trivial amount of IPv6.

A6-d) You should fix that. We see on our tool IPv6 attacks.

Q7) Do you consider important adding visibility for rules affecting a particular peer between users? For example, if the attack is coming from another NREN?

A7-a) It isn't worth it. Happens once a year and needs so much coding.

A7-b) Good thing to have.

A7-c) We think it is very important.

A7-d) Useful feature but not high priority.

Q8) How useful would you consider the ability to download attack reports (PDF, excel etc. format) depicting in detail the nature of the attack in bytes/packets in the scale of 1-3 (1 being least important, 3 very important).

A8-a) Totally, very important (mark as 3). Finding very lacking currently. Add longer time frame, like 6 months.

A8-b) 3. Very useful

A8-c) Very interesting and important. 3.

A8-d) Very important. Maybe we should ask other NRENs how they expect the reports.

Q9) Do you recall any time that FoD failed your expectations? Can you elaborate and recommend how to overcome that issue in the future?

A9-a) No. FoD has lived up to its expectation all the time, and is what we need.

A9-b) Don't recall.

A9-c) All good.

A9-d) One or two times the service was not available.

Q10) Do you have any recommendations for FoD's general improvement? It could include GUI and other functionalities of it (e.g. filtering/searching for rules).

A10-a) Really interesting is the scrubbing centre. And we are willing to pay for it.

A10-b):

- At the dashboard, username is shown by eduGAIN cryptic identifier. Would like to see this is in human format i.e. First Name, Last Name. (This is already going to be covered by an update for FoD v1.5 ready nearly to be released productively).
- Filtering searching rules sounds good, especially explicitly by IPAddress+Port
- Also would like to keep the rule data for more than a year.
- At the moment there are problems with statistics which use IP fragment option filtering
- (This is already going to be covered by an update for FoD v1.5 that is nearly ready to be released in production)

A10-c) No improvement.

A10-d) Registration of the users that can be done by admin NREN CERT users themselves that would not require GÉANT staff.

3.2 Analysis of User Study Results – Prioritisation

A comparison and analysis of the answers of the interviews listed in the previous section was performed.

The outcome per question is given below.

Features and functions specified in the questions Q1-Q10 were named F1-F10 to make it easier to reference them later.

Q1: feature "FoD as single interface for different mitigation technologies beyond BGP FlowSpec" (F1) definitely wanted

Q2: feature "BGP FlowSpec propagation via BGP" (F2) medium priority

Q3: feature "docker image for test installation" (F3) medium priority

Q4: feature "REST API" (F4) low priority

Q5: feature "web application firewall" (F5) very low priority

Q6: feature "rules for IPv6 traffic" (F6) wanted in the long term

Q7: feature "visibility of rules affecting own network" (F7) medium priority

Q8: feature "pdf/excel reporting" (F8) definitely wanted

Q9: no major issues in the past with FoD

Q10: various individual, different ideas for improvement:

- better, explicit filtering by IP addresses+TCP/UDP port (F10a)
- statistics beyond a month, up to a year and beyond (F10b)
- master-user interface for administering own logins of a user's network (F10c)

Compiling these results yields the following priority-sorted plan for FoD improvements/enhancements based on user assessment:

- High priority: F1 and F8
- Medium priority: F2, F3, F7; F6 (long-term)

- Low priority: F4, F10a-10c
- Very low priority: F5

In addition to these user-assessed features and functionalities, integration of FoD and NEMO (Int-NEMO), i.e. cooperation with Task WP8 T3.3 is high priority.

The relationship between the features F1-F10 and Int-NEMO to the original four areas (A1-A4) derived from the Description of Work (see Section 2.5) and is provided for completeness here:

A1: Int-Nemo (high), F2 (medium), F3 (medium), F4 (low)

A2: Int-Nemo (high), F8 (high), F7 (medium), F10b (low)

A3: F1 (high)

A4: F5 (very low)

General: F6 (medium long-term), F10a (low), F10c (low)

References

[FlowSpec]	P. Marques, N. Sheth, R. Raszuk, B. Greene, J. Mauch and D. McPherson, *Dissemination of Flow Specification Rules*, August 2009
[D8.2]	https://www.geant.org/Projects/GEANT_Project_GN4/deliverables/D8.2_Firewall-on-Demand-Progress-Report.pdf
[D8.3]	https://www.geant.org/Projects/GEANT_Project_GN4/deliverables/D8.3_Distributed-Denial-of-Service-Mitigation-v1.0-Pilot.pdf
[D8.12]	https://www.geant.org/Projects/GEANT_Project_GN4/deliverables/D8.12_Distributed%20Denial%20of%20Service%20Mitigation%20v1.0%20Pilot%20Follow-up.pdf
[GnFoD]	https://github.com/GEANT/FOD
[Idea]	https://idea.cesnet.cz/en/index
[NSHaRP]	http://geant3.archive.geant.net/Network/NetworkOperations/Pages/NSHaRP-NetworkSecurity.aspx
[Redirect]	J. Haas, *Clarification of the Flowspec Redirect Extended Community*, October 2015
[RepShield]	https://www.cesnet.cz/wp-content/uploads/2015/12/Reputation-Shield-BARTOS.pdf
[Warden]	https://warden.cesnet.cz/

Glossary

FoD	Firewall on Demand
DDoS	Distributed Denial of Service
NOC	Network Operations Centre
NSHaRP	Network Security Handling and Response Process
BGP	Border Gateway Protocol
FRU	Firewall Rule Updater
CERT	Computer Emergency Response Team
SOC	Security Operations Centre