12-07-2017

Deliverable D8.2
Firewall-on-Demand Progress Report

Deliverable D8.2

Contractual Date:	31-08-2017
Actual Date:	12-07-2017
Grant Agreement No.:	731122
Work Package/Activity:	8/JRA2
Task Item:	Task 6
Nature of Deliverable:	REPORT (R)
Dissemination Level:	PU (Public)
Lead Partner:	DFN (LRZ)
Document ID:	GN4-2-17-42E03
Authors:	David Schmitz, Jerry Sobieski (Nordunet), Ivana Golub (PSNC)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Abstract
This document describes the work carried out in the GN4-2 Joint Research Activity "Network Services Development" (JRA2)– Network Security Task (Task 6) reporting on the Firewall on Demand version 1.5 service within the GEANT network environment.

Table of Contents

Table of Figures

Executive Summary

This document supports the work carried out in the Network Security task (Task 6) in Network Services Development Joint Research Activity (JRA2) of the GN4 Phase 2 (GN4-2) project for the next version of Firewall on Demand (FoD). FoD service development, started by GRNET during GÉANT3plus, entered production in version 1.1.1 during GN4-1. FoD is a BGP-FlowSpec-based [rfc5575] (D)DoS mitigation solution, whose users are National Research and Education Network (NREN) Network Operation Centres (NOCs).

In GN4-2, the development of FoD is continued in cooperation with GRNET and according to GÉANT and NREN requirements. It starts with the assessment of possible areas for improvement for the existing version, enhancements of BGP FlowSpec-based FoD in the next version (v1.5), and then continues with the short-, mid- and long-term plans for the development of FoD, including a next generation of this service, Firewall as a Service (FwaaS). FwaaS is envisioned as a SDN/NFV-based (D)DoS-mitigation solution for GÉANT, NRENs and other institutions, which will allow fine-grained, accurate, and distributed (D)DoS mitigations beyond BGP FlowSpec, with the possibility of delegation.

FoD v1.5 entered pilot phase evaluation 1 July 2017, within the GÉANT core network. A limited set of GÉANT NREN subscribers are able to utilise the v1.5 tool to set and/or manage firewall rules in GÉANT core routers to mitigate DDoS attacks before those flows converge to saturate NREN and/or campus network links [PILOT]. Version 1.5 will remain in pilot mode until 1 October 2017, and barring any unforeseen issues revealed during the pilot, will be upgraded to be production status as of that date.

1 Introduction

Firewall on Demand (FoD) is a BGP-FlowSpec-based [rfc5575], (D)DoS mitigation solution that was previously developed by GRNET as part of an earlier phase of the GÉANT project, GÉANT3plus [FLOWSPY]. FoD is currently provided in the GÉANT core network to allow users (NREN NOC administrators) to administer BGP FlowSpec rules via a web interface. This allows normally routed GÉANT IP traffic to be filtered, based on the administered BGP FlowSpec rules [rfc5575] [rfc7674].

In the rest of this document, Section 2 covers basic information about FoD and details the status of FoD at beginning of GN4-2, In Section 3 changes and enhancements of FoD performed during the first 13 months of GN4-2 are described, while Section 4 covers planned changes in the upcoming months. Section 5 outlines long-term plans to extend FoD beyond the BGP FlowSpec rules, based on SDN/NFV techniques or support for vendor DDoS solutions.

2 Status of FoD at the Beginning of GN4-2

Firewall on Demand (FoD) provides a mechanism to mitigate large-scale network attacks, e.g. (D)DoS, through propagation of BGP FlowSpec rules. For simple rule configuration, a web-based interface capable of crafting and disseminating/withdrawing FlowSpec rules 'on demand' has been provided. The reason why FlowSpec is preferred to other tools is the speed with which it provides, on top of the granularity that can be given to a firewall rule, as compared to older DDoS mitigation techniques, such as access control lists (ACLs) and remotely triggered black hole (RTBH) filtering.

More about the application, its functionalities, and its software architecture can be found by project participants in GN4-1 deliverable *D7.1 Multi-Domain Service Security Architecture* (SA3 T1) [GN4-1_D7-1].

At the beginning of GN4-1, v1.1.1 was used in production in the GÉANT core network. It has been recognised that this version has some space for improvement, e.g.:

- Rules could be entered automatically (e.g. a rule control API).
- Support for specification of port ranges could be added to rule editing interface.
- More flexible rate limiting can be enabled (currently only three, fixed choices for bandwidths are available - 1k, 10k and 100k).
- Provide feedback about the effectiveness/effect of rules available, e.g. by statistics graphs of dropped/rate-limited packets over time.
- Enable internal logging of FoD user actions.
- Replace current communication to the router(s) is via NETCONF, with BGP (e.g. with EXABGP) [EXABGP].
- Enable support for IPv6 (at present, limitation exists on router platform in GÉANT core).

The first actions on the further development of FoD service are based on the analysis and prioritisation of the recognised improvement opportunities, taking into considerations feedback from FoD users. The next version, v1.5, is still based on BGP FlowSpec, until a more flexible, DDoS mitigation solution is available, covering more types of DDoS attacks and including support for SDN/NFV.

3 Enhancements and Improvements to FoD: v1.5

At the beginning of GN4-2, JRA2 T6 performed two tasks related to the future development of FoD: JRA2 T6 formed a DDoS detection/mitigation working group and started to build upon the existing BGP FlowSpec v1.1.1 to grow it into the new v1.5.

3.1 DDoS Detection/Mitigation Working Group

JRA2 T6 gathered requirements from current and potential FoD users from the GÉANT community in order to verify the requirements given in the GN4-2 Description of Work [DoW], as well as to consider the available feedback for future work and development for FoD and planned a new Firewall as a Service solution.

An informal DDoS detection/mitigation working group (DDoS D/M WG) was formed, consisting of relevant JRA2 T6 members, but also non-task members from different NRENs, including: SURFnet, GARR, and since March 2017, DEIC. The WG conducted a survey about DDoS detection/mitigation, covering the whole GÉANT community, and discussed potential DDoS detection/mitigation approaches and solutions, commercial and open source.

The survey respondents included network engineers, security engineers, as well as managers from 19 NRENs. Although a thorough analysis of this survey is still outstanding, summary points are as follows:

- FoD is well known to all (responding) NRENs.
- Most of those NRENs use NetFlow-based DDoS detection, similarly as GÉANT uses FlowMon [FLOWMON] with NSHaRP [NSHaRP].
- A GÉANT-provided 'scrubbing-centre solution' providing data cleansing station to analyse and remove malicious traffic is desired by most of the responding NRENs (71.4%).
- Further collaboration with other NRENs is desired via experience sharing (33.3%) or even common development (38.9%).

The survey results revealed that in the short-to mid-term, there is a need to add missing functionality to BGP FlowSpec-based FoD in order to make it easier to use. Long-term design and development of an SDN/NFV-based replacement, Firewall-as-a-Service (FwaaS), based either on open source or commercial solutions, is consistent with user requirements.

3.2 FoD Development

Initial activity in JRA2 T6 involved getting acquainted with FoD's software architecture and its code, as well as connecting with GRNET. GRNET developers continued to develop FoD, primarily for their single-domain purposes. However, due to the common goals of JRA2 T6 and GRNET, both teams will coordinate their work to avoid duplication of effort.

The GRNET version is available on GitHub [FLOWSPY], which contains a REST API for querying and controlling BGP FlowSpec rules. Since providing a REST API for automated rule proposal was on the list of needed functionalities in JRA2 T6, the team decided to test this existing GRNET version v1.3 with the desired functionality and build further development on this version. Testing was carried out with real traffic over the connected router on the second testing machine.

The enhancements and improvements of FoD carried out in JRA2 T6 during the first 13 months of GN4-2 comprise the following new functions:

- Capability to specify source/destination port ranges in BGP FlowSpec rules [rfc5575].
- Statistical graphs for active FlowSpec rules over time.

The new version of FoD enhances the forms for adding new rules as well as changing existing rules. Figure 3.1 shows an example of the Add rule form with an example specification of source/destination port ranges mixed with single port values.

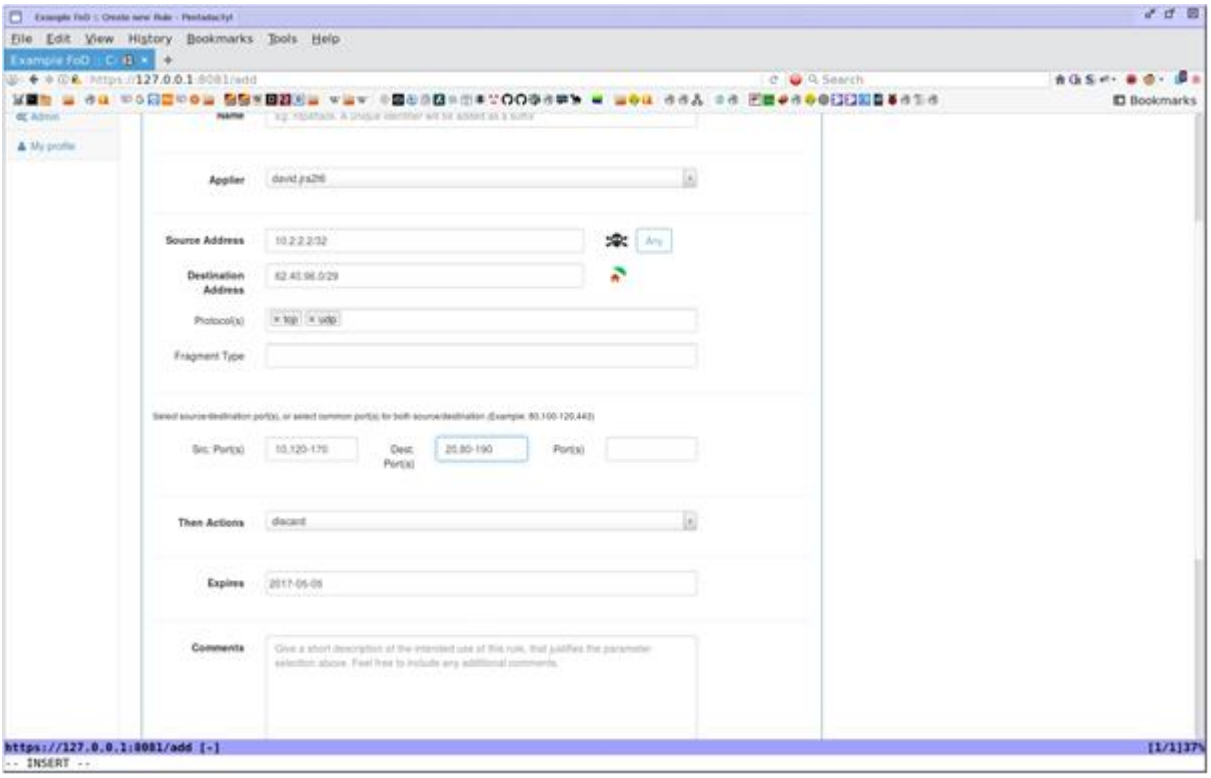

Figure 3.1: Example of Add Rule Form with capability to specify source/destination port ranges

The GRNET developer group also provided JRA2 T6 with the code of a FoD graph plugin they developed, and use-per-rule over time (of dropped/rate-limited packets) to integrate statistics.

In order to be able to gather SNMP data and visualise data gathered from FoD, JRA2 T6 started to develop a module that was able to:

- Collect SNMP statistics from all BGP FlowSpec-enabled routers.
- Store and prepare visualisations as PNG images.
- Provide all PNG images via a REST-API to the FoD graph plugin.

Figure 3.2 shows the new functionality.

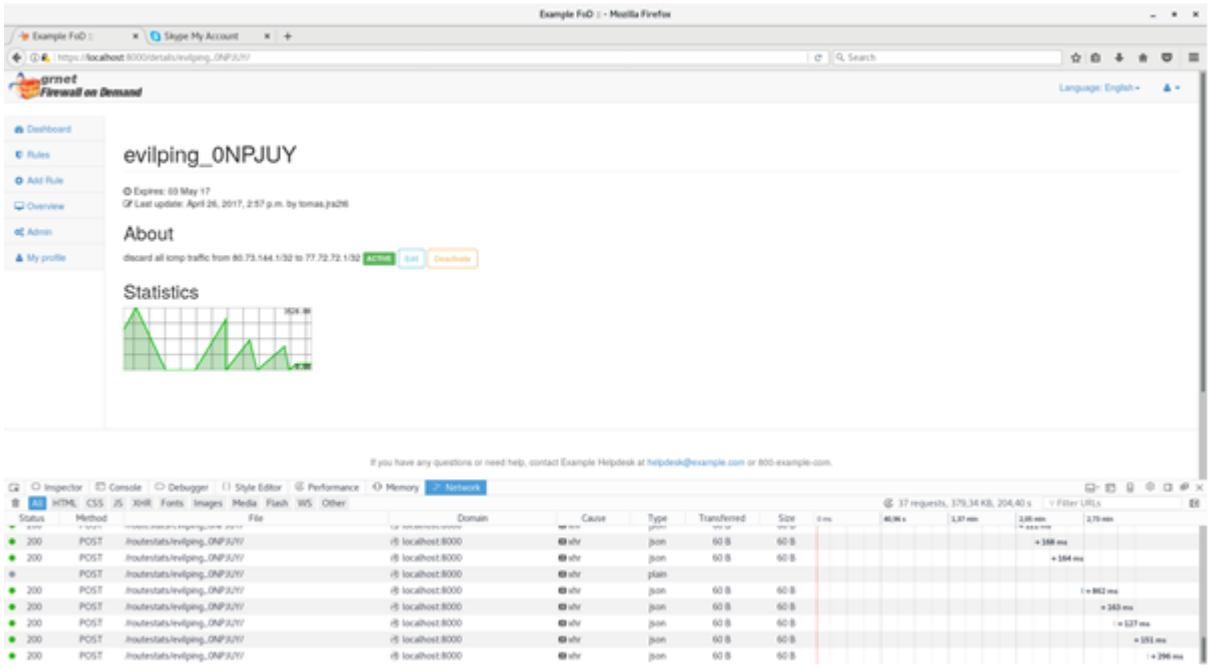

Figure 3.2: Example of statistics view of a mitigation rule

This new version of FoD includes the first planned improvements and is able to filter traffic based, not only on IP ranges, but also on port ranges, and to gather more statistics than what is available with the current production version. The next step will be to test this version with selected users and then to prepare this version for production together with the Service Activity 2 Trust and Identity and Multi-Domain Services (SA2) team responsible for operation of the GÉANT core network in production.

4 Planned Short-to-Mid-Term Changes for FoD

The clear goal for the mid-term (by October 2017) is to provide an automated rule proposal, generated from NSHaRP events about DDoS attacks. For quality assurance, this will be carried out via the Rep(utation)Shield [REPSHIELD], developed in CESNET as part of JRA2 T6. Before the RepShield is developed , the rules may be initially generated directly from NSHaRP events.

JRA2 T6 and GRNET teams have also planned to test FoD with a virtual test router provided by GRNET, which supports IPv6 regarding BGP FlowSpec.

Additional short- to mid-term functions that may also be added include:

- More flexible rate limiting.
- Internal logging of FoD user actions.
- Exchanging the NETCONF interface to the router with BGP, possibly introducing an abstraction layer for different interfaces/technologies, also with respect to long-term SDN/NFV/vendor-based filtering techniques beyond BGP FlowSpec.

Furthermore, it is expected that FoD will not only be used in the GÉANT core, but also tested in an NREN as an single-domain solution. Regarding this, the difference concerning use cases/user stories will have to be analysed and appropriately aligned with the aforementioned developments.

In the slightly longer-term, FoD service integration with Service Provide Architecture (SPA) could be considered. SPA is a result of work in JRA2 T2, and it considers support for business processes, based on Operations Support Systems (OSS) and Business Support Systems (BSS) by TMF Forum [OSSBSS], [TMFORUM].

The next GN4-2 deliverable, *D8.3 Distributed Denial of Service Mitigation v1.0 Pilot* will follow-up on the reporting of some of the short/mid-term changes carried out on (BGP FlowSpec-based) FoD, especially the planned automated rule proposal functionality. A detailed roadmap for FoD is provided in the JRA2 T6 Milestone document *M8.6. Network Security Services Roadmap* [GN4-2_M8.6], available for GÉANT project members.

5 Firewall as a Service as a Future FoD Solution

In the long-term, it is expected that FoD will be replaced or enhanced by a DDoS detection/mitigation solution. In addition to traffic filtering based on BGP FlowSpec and source/destination port/protocol/IP address range-based traffic selection, this would also allow more accurate determination of unwanted traffic for mitigation of certain types of DDoS attacks. This enhanced version of FoD is Firewall-as-a-Service (FwaaS).

FwaaS will be based on SDN/NFV-techniques, with the possibility of also including vendor-specific DDoS mitigation solutions. Candidates for vendor-solutions to support this include:

- A10 mitigation box, which is currently on test in the GÉANT core [A10].
- CORSA NSE-7000 box [CORSANSE7000].
- Hardware cards for traffic filtering currently developed by CESNET.

Apart from additional functionalities, such solutions promise the possibility of delegating DDoS mitigation control among GÉANT, NRENs, and institutions.

The design for FwaaS will also include consideration and analysis of related existing or draft standards, including, but not limiting to, the following related IETF standards and drafts:

- I2NSF: Interface To network security functions: [NSF_CAPABILITIES] [NSF_INTERFACE] [NSF_SECURITY] [NSF_STATEMENT] [NSF_USECASES] [NSF_DDoS] [NSF_CLOUD] [NSF_ARCH].
- SFC: Service Function Chaining [rfc7665] SFC and Overlay network [OVERLAY].
- DOTS: DDoS Open Threat Signalling [DOTS]. This analysis will be also be carried out in cooperation with the JRA1, T2 team.

This long-term design and development of FwaaS will depend on the feedback from the community on the current developments, on the further development of GÉANT and the NRENs' plans in the area of network security, and the development of industry standards and best practices. It will also depend on the available manpower in this and in future GÉANT projects.

6 Conclusions

This document presents the work of Task 6: Network Security, in the Network Services Development Joint Research Activity (JRA2) of GN4-2 project, specifically, the development of the Firewall on Demand service. Although the service has been in production for some time, room for improvement is recognised by the original developers, as well as by the JRA2 T6 team and FoD users.

Initial improvements have been achieved in the area of more specific traffic filtering. In addition to the source/destination port/protocol/IP address based filtering, the new version of FoD allows port-based filtering, which enables more specific determination and selection of the unwanted traffic. In addition, improvement has been made in the statistics of completed traffic filtering.

In the longer term, the battle with DDoS attacks will continue in the area of SDN/NFV, in the addition of other stand-alone open-source and/or commercial software tools, and in consulting active standardisation and best-practice efforts for the need and benefit of GÉANT community.

References

[A10]	Amazon.com, Server Load Balancers | Application Delivery | DDoS Mitigation | A10, Apr 2017
[CLOUDFLARE]	CloudFlare, TM Forum - The Roadmap to Digital Success, Apr 2017
[CORSANSE7000]	Level 3 Communications, nse7000-network-security-enforcement - Open Networking Foundation, Apr 2017
[DJANGO]	www: Rackspace Hosting, The Web framework for perfectionists with deadlines | Django, Apr 2017
[DOTS]	Mortensen, A., Andreasen, F., Reddy, T., Gray, C., Compton, R. and Teague, N., Distributed-Denial-of-Service Open Threat Signalling (DOTS) Architecture, Jul 2016.
[DoW]	gn42dow20151218: GÉANT GN4-2, SGA2 Description of Work, 2015.
[EXABGP]	Exa-Networks/exabgp: The BGP Swiss army knife of networking, May 2017 https://github.com/Exa-Networks/exabgp
[FLOWMON]	Master Internet s.r.o, Flowmon.com, Nov 2016, http://www.flowmon.net
[FLOWSPY]	GRNET Firewall on Demand platform. Powers, Aug 2016, https://github.com/grnet/flowspy.
[SRC_CODE_REVIEW]	GÉANT GN4-2, SA2-T1, FoD validation - source code review, Aug 2016
[GN4-1_D7-1]	Metzger, S. (LRZ), Bartos, V. (CESNET), Nussbacher, H. (IUCC) and Spatharas, E. (GÉANT), D7.1 Multi-Domain Service Security Architecture, April 2016.
[GN4-2_M8-6]	https://intranet.geant.org/gn4/2/Activities/JRA2/Milestones%20Documents/Network%20Security%20Services%20Roadmap/M8.6_Network-Security_Roadmap.pdf
[NSF_ARCH]	Hyun, S., Woo, S., Sungkyunkwan University, Jeong, J. and Park, J.-S., Service Function Chaining-Enabled I2NSF Architecture, Jul 2016.
[NSF_CAPABILITIES]	Basile, C., and Lopez, D., A Model of Security Capabilities for Network Security Functions, Jul 2016.
[NSF_CLOUD]	Hares, S. and Robert Moskowitz, R., Inter-Cloud DDoS API Yang Model, Jul 2016.
[NSF_DDoS]	Fang, L., and Bansal, D., Inter-Cloud DDoS Mitigation API, Mar 2016.

[NSF_INTERFACE] Lopez, E., Lopez, D., Dunbar, L., Strassner, J., Zhuang, X., Parrott, J.,Krishnan, R., Durbha, S., Kumar, R. and Lohiya, A., Framework for Interface to Network Security Functions, Aug 2016.

[NSF_SECURITY] Jeong, J., Kim, H., Park, J.-S., Ahn, T.-J., Sungkyunkwan University and Korea Telecom, Software-Defined Networking Based Security Services using Interface to Network Security Functions, Jul 2016.

[NSF_STATEMENT] Dunbar, L., Zarny, M., Jacquenet, C., Boucadair, M., and Chakrabarty, S., Interface to Network Security Functions (I2NSF) Problem Statement, May 2015.

[NSF_USECASES] Hares, S., Dunbar, L., Pastor, A., Lopez, D., Zarny, M., Leymann, N., Georgiades, M., Minpeng Qi, M., Boucadair,M., Jacquenet, C., and Chakrabarty, S., I2NSF Problem Statement and Use cases, Dec 2015.

[NSHaRP] GEANT Limited, NSHaRP, Aug 2016, http://geant3.archive.geant.net/Network/NetworkOperations/Pages/NSHaRP-NetworkSecurity.aspx.

[OSSBSS] Zen Internet Ltd, The Definition of OSS and BSS | OSS Line, Apr 2017

[OVERLAY] Ao T., Interworking SFC Network and Overlay network, Mar 2016.

[PILOT] NRENs participating in FoD v1.5 pilot include: RedIRIS, LITnet and EEnet.

REPSHIELD] CESNET z.s.p.o., Aug 2016, https://www.cesnet.cz/wp-content/uploads/2015/12/Reputation-Shield-BARTOS.pdf.

[rfc5575] Marques, P., Sheth, N., Raszuk, R.,Greene, B.,Mauch, J. and McPherson, D.,Dissemination of Flow Specification Rules, August 2009.

[rfc7665] Halpern J., and C. Pignataro, C. Service Function Chaining (SFC) Architecture, October 2015.

[rfc7674] Haas, J., Clarification of the Flowspec Redirect Extended Community, October 2015.

[TMFORUM] https://www.tmforum.org/

Glossary

ACL	Access Control List
API	Application Programming Interface
BGP	Border Gateway Protocol
BSS	Business Support Systems
DDoS	Distributed Denial of Service
DOTS	DDoS Open Threat Signalling
DoW	Description of Work
FoD	Firewall on Demand
FWaaS	Firewall as a Service
GN4-2	GÉANT Network 4, Phase 2 project, part-funded from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No.731122
I2NSF	Interface to Network Security Functions
JRA	Joint Research Activity
NFA	NetFlow Analyzer
NFV	Network Function Virtualisation
NOC	Network Operation Centres
NREN	National Research and Education Network
OSS	Operations Support Systems
PLM	Project Lifecycle Management
PNG	Portable Network Graphics
REST	Representational state transfer
RTBH	Remotely Triggered Black Hole
SA	Service Activity
SDN	Software Defined Network
SFC	Service Function Chaining
SGA	Single Grant Agreement
SPA	Service Provider Architecture
SNMP	Simple Network Management Protocol
T	Task