

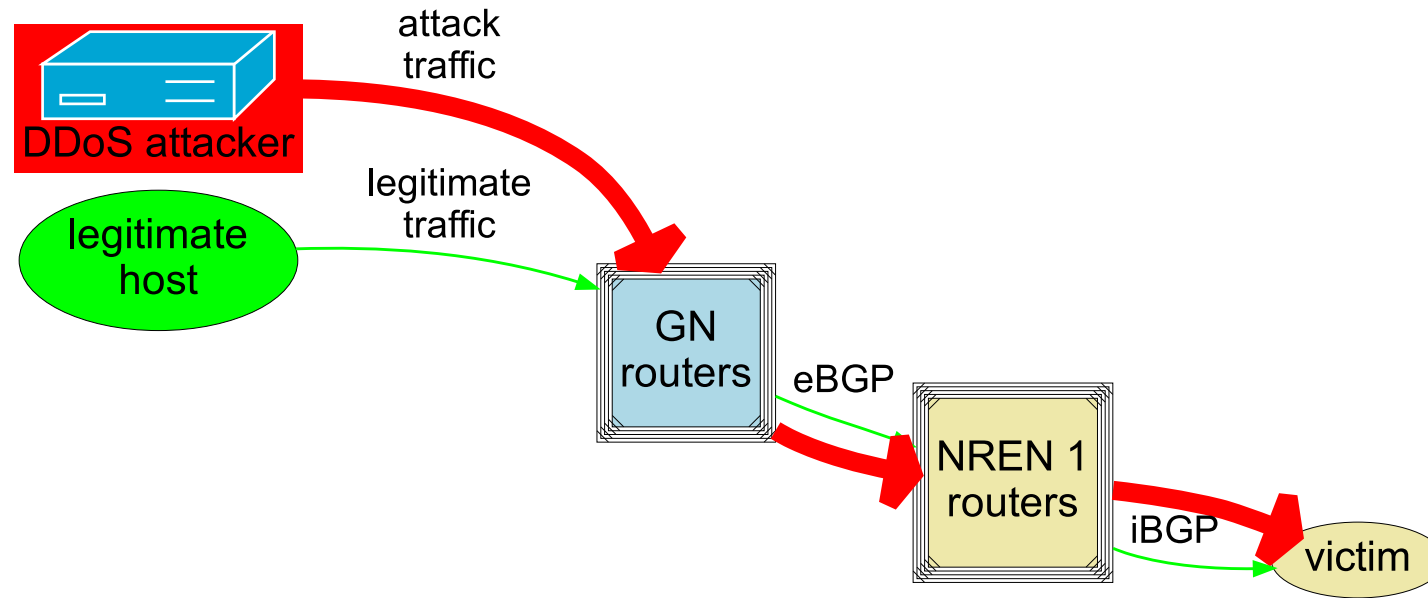
Relying on RARE for DDoS Attack Protection - Demonstrating RARE Integration with GÉANT DDoS Attack Protection Services (FoD and NeMo Use Cases)

Nikos Kostopoulos, David Schmitz

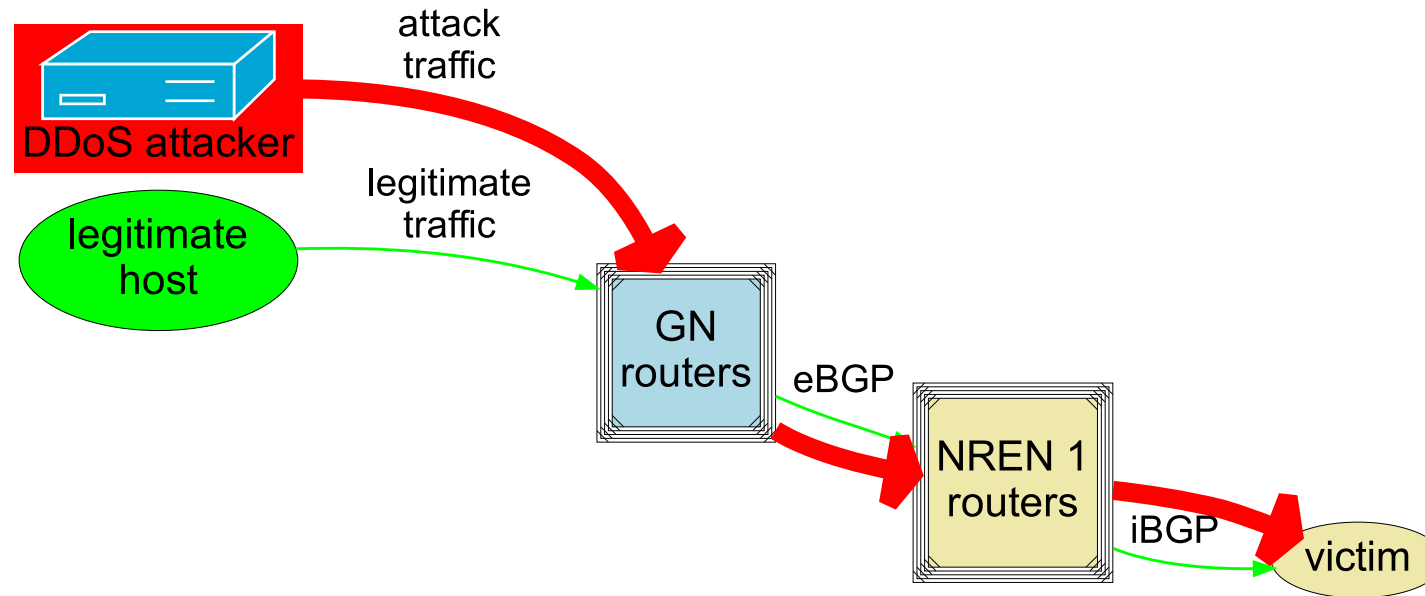
08.12.2023

www.geant.org

DDoS-Attack (1)



DDoS-Attack (2)



- **Victim host attacked by DDoS**
- **Victim's local network may also be impacted ?**

FoD and NeMo with freeRTR: DDoS detection and mitigation demo

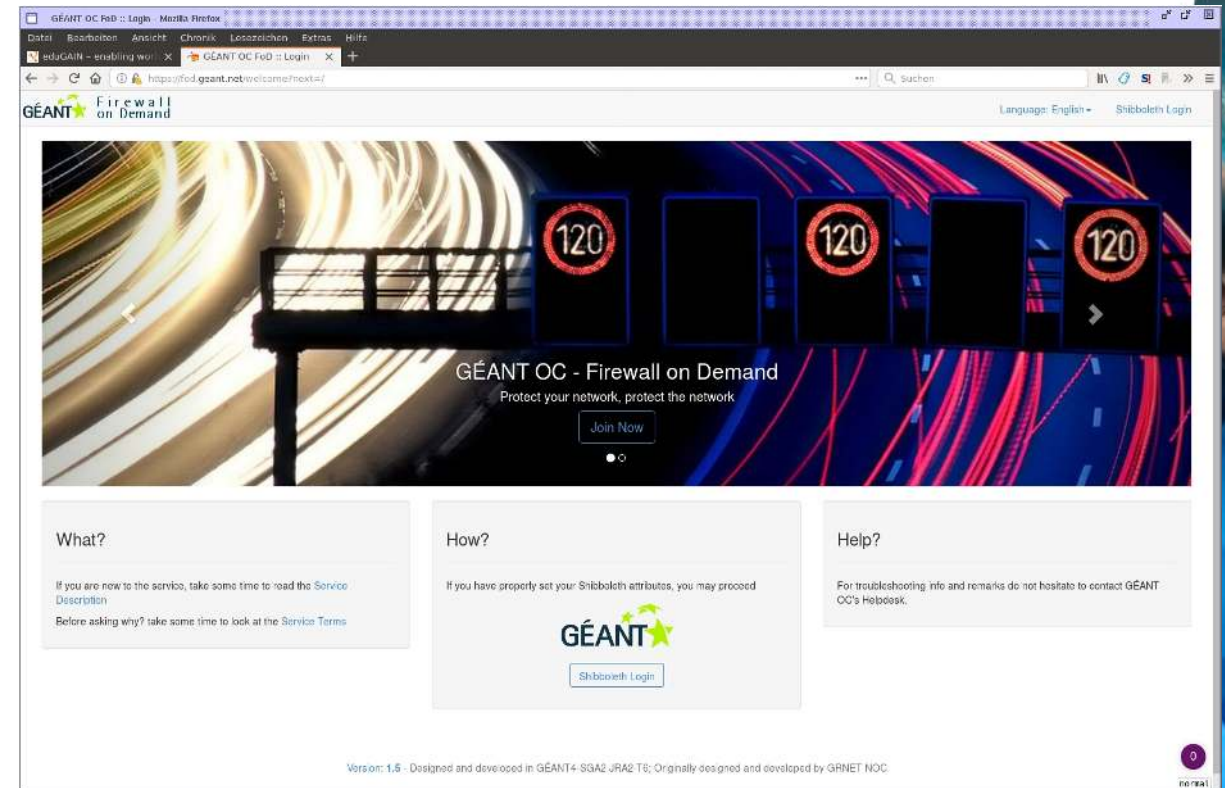
- Firewall-On-Demand (FoD): own DDoS mitigation by the user via BGP FlowSpec
- NeMo: DDoS detection and mitigation
- freeRTR
 - emulation and demo-ing of CISCO-like router(s)
 - also used in real hardware



Firewall-On-Demand (FoD)

Firewall-On-Demand (FoD): Introduction

- not 'Firewall' in the usual sense!
- service for DDoS mitigation control by user himself
 - dynamically, on the routers
 - BGP FlowSpec-based
 - multi-tenant, eduGAIN-based
 - developed by GÉANT project
- z.B. GÉANT FoD service instance
 - mitigation within GÉANT core
 - for NREN NoC Admins
 - productive since > 8 years
- GÉANT WP8-T3-DDoS
 - Continued development and support
 - Collaboration with the GÉANT security team



Firewall-On-Demand (FoD): Benefit for Users

- user (NREN NoC) is able to perform DDoS mitigation
 - for own IP traffic: start/edit/stop
 - manually (WebUI) oder automated (REST API)
 - without contacting GÉANT NoC

- ⇒ flexible, independent, fast mitigation
(most DDoS attacks: < 1 h)

Firewall-On-Demand (FoD): Input of a mitigation rule

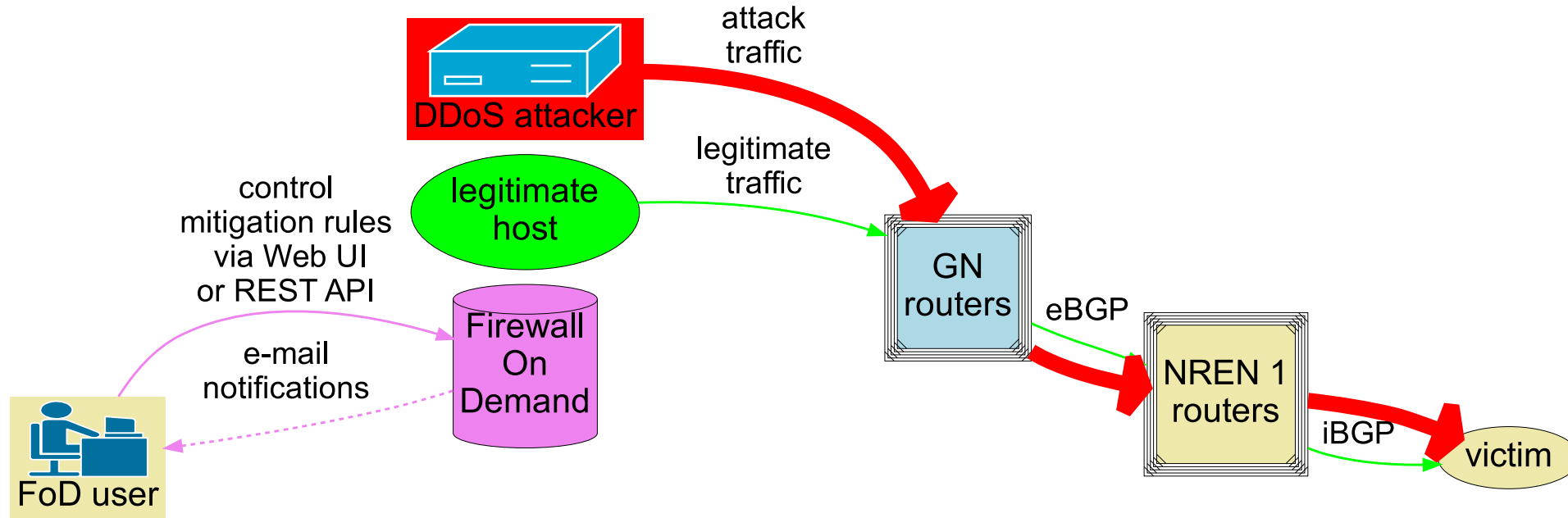
The screenshot shows the 'Edit rule: testrule2_PHL8L' page in the GEANT OC FoD web interface. The page is titled 'Firewall Rule' and contains the following configuration fields:

- Applier:** admin
- Source Address:** 0.0.0.0/0 (with a skull and crossbones icon and an 'Any' button)
- Destination Address:** 12.11.10.12/32 (with a house icon)
- Protocol(s):** udp
- Fragment Type:** (empty field)
- Select source/destination port(s), or select common port(s) for both source/destination (Example: 80,100-120,443):**
 - Src. Port(s):** 1000-2000;
 - Dest. Port(s):** 3000-4000;
 - Port(s):** (empty field)
- Then Actions:** rate-limit:10000k
- Expires (YYYY-MM-):** 2021-08-21

The interface also features a sidebar with navigation options: Rules, Add Rule, Overview, Admin, and My profile. The browser address bar shows the URL: https://test-fodd-lab-1.geant.net/edit/testrule2_PHL8L.

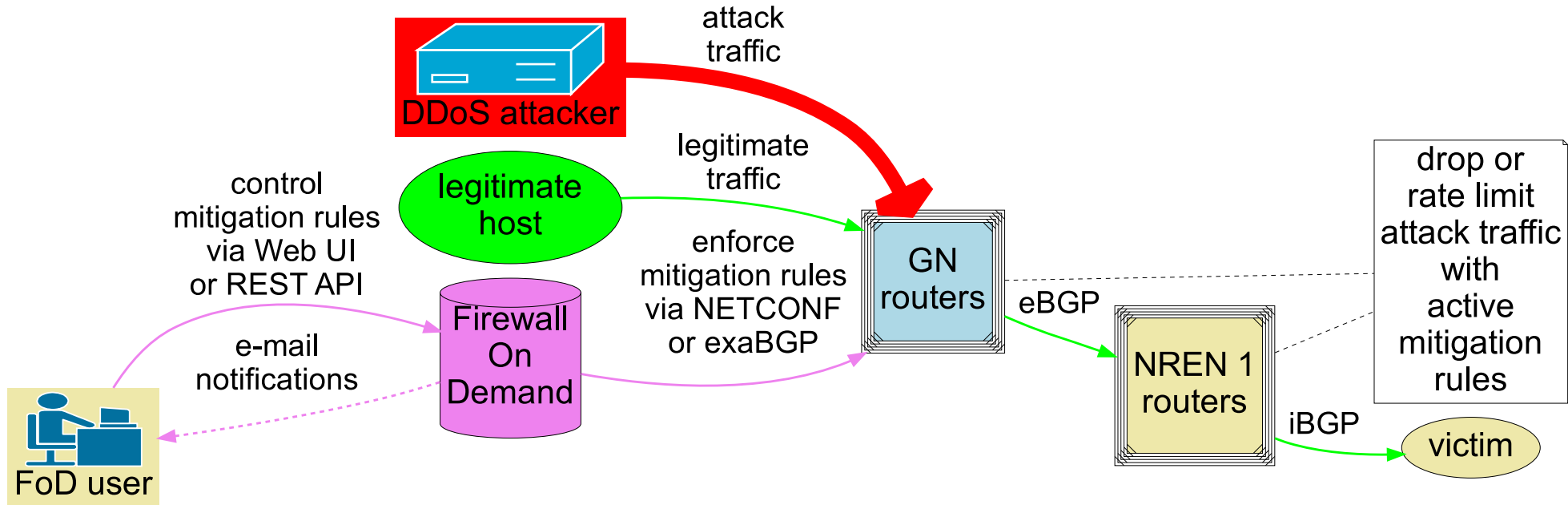
- **Match**
 - source IP prefix (attacker)
 - destination IP prefix (multi-tenant)
 - IP protocol: ICMP, UDP, TCP
 - ggf. UDP/TCP port (lists)
 - IP fragment options
- **Mitigation**
 - drop all
 - rate limit
- **Expire time**

Firewall-On-Demand: Mitigation



- **Victim host attacked by DDoS**
- **Victim's local network may also be impacted**

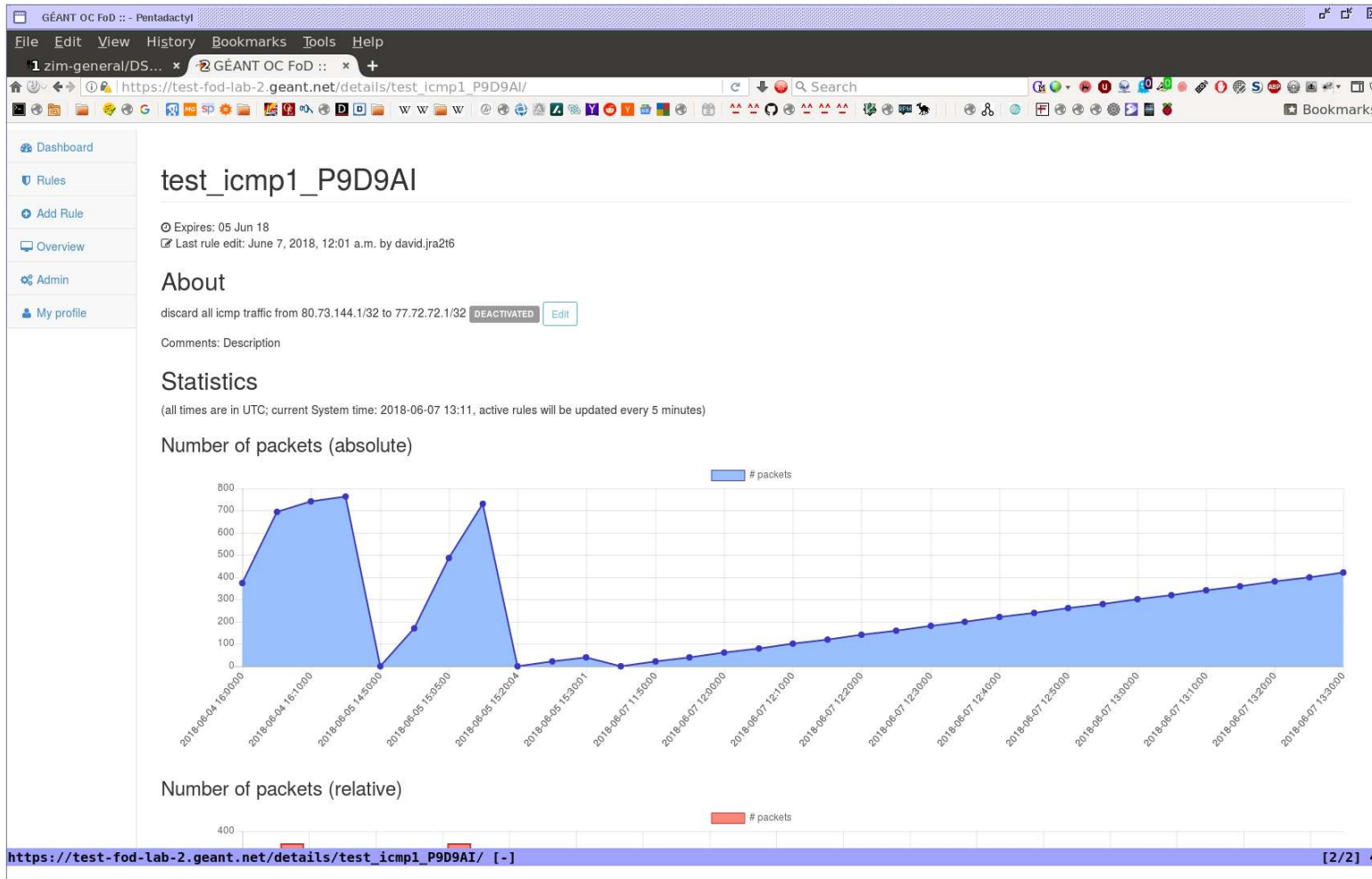
Firewall-On-Demand: Mitigation



- **DDoS traffic blocked as early as possible**
- **Based on BGP FlowSpec supported in routers**



Firewall-On-Demand (FoD): Statistics of a mitigation rule



actually dropped
bytes / packets

via SNMP
(JUNOS-specific filter stats via
Firewall MIB)
from routers, aggregated

Firewall-On-Demand (FoD): Overview of the mitigation rules

The screenshot shows the GÉANT Firewall On Demand (FoD) web interface. The browser address bar shows the URL `https://test-fodd-lab-1.geant.net`. The page title is "My rules". The left sidebar contains navigation links: Dashboard, Rules, Add Rule, Overview, Admin, and My profile. The main content area displays a table of Firewall Rules. The table has columns for Name, Match, Then, Status, Applier, Updated, Expires, Response, and Actions. Three rules are visible: testrule1_8FZALJ (DEACTIVATED), testrule2_9SOBCQ (DEACTIVATED), and testrule2_PHLD8L (ACTIVE). The right sidebar contains Shortcuts (Add Rule, My Profile) and Live status (logs of rule edits).

My rules

20 records per page

ACTIVE PENDING ERROR

DEACTIVATED

Showing 1 to 5 of 5 entries (filtered from 8 total entries)

Name	Match	Then	Status	Applier	Updated	Expires	Response	Actions
testrule1_8FZALJ	Dst Addr: 12.11.10.10/32 Src Addr: 0.0.0.0/0 Protocols: icmp	rate-limit 100k	DEACTIVATED	admin (null)	2021-07-23 09:14:54	2999-01-01	Rule expired	Reactivate
testrule2_9SOBCQ	Dst Addr: 12.11.10.12/32 Src Addr: 0.0.0.0/0 Protocols: udp DstPorts: 3000-4000,5000-6000 SrcPorts: 1000-2000,3000-4000	rate-limit 10000k	DEACTIVATED	admin (null)	2021-07-23 09:15:05	2021-08-21	Rule expired	Reactivate
testrule2_PHLD8L	Dst Addr: 12.11.10.12/32 Src Addr: 0.0.0.0/0 Protocols: udp DstPorts: 3000-4000,5000-6000 SrcPorts: 1000-2000,3000-4000	rate-limit 10000k	ACTIVE	admin (null)	2021-07-23 09:15:13	2021-08-21	Successfully committed	Edit Deactivate

Shortcuts

- Add Rule
- My Profile

Live status

- 2021-08-09 12:23:33
admin: Rule edit: testrule2_QEDV2H - Result: NETCONF connection failed
- 2021-08-09 12:22:44
admin: Rule edit: testrule2_BDQSGQ - Result: NETCONF connection failed
- 2021-08-09 12:21:37
admin: Rule edit: testrule2_K8A25Z -

normal



"FoD in a box" using Docker Compose

- Docker based-container running FoD inside
 - as reference installation
 - for testing
- Docker Compose specification for FoD container, Freertr router, attacker and victim host containers
 - https://github.com/GEANT/FOD/blob/feature/exabgp_support2/docker-compose-singlefodctr-novol.yml
- instructions how to build and use Docker Compose specification manually
 - https://github.com/GEANT/FOD/blob/feature/exabgp_support2/docker-compose/README.txt
- automated FoD Mitigation Demo (based on Docker Compose)
 - demo script:
https://github.com/GEANT/FOD/blob/feature/exabgp_support2/docker-compose/demo1.sh

"FoD in a box" using Docker Compose: Automated Mitigation Demo

- runs only in terminal, not via Web UI
- rules emitted into FoD via Python code

Demo

"FoD in a box" based on Containerlab

- Containerlab (<https://containerlab.dev/>)
 - similar as Docker Compose, but more network-centric
 - typically prebuild containers for testing specific network components (e.g., routers, freeRTR, FoD, etc.) are used
- Containerlab specification for FoD with freeRTR:
 - <https://github.com/rare-freertr/freeRtr-containerlab/blob/main/lab/005-rare-hello-fod/rtr005.clab.yml>
- Automated FoD Mitigation Demo (based on Containerlab)
 - instructions for manual demo: <https://github.com/rare-freertr/freeRtr-containerlab/blob/main/lab/005-rare-hello-fod/containerlab-fod-freertr.txt>
 - demo script:
<https://github.com/rare-freertr/freeRtr-containerlab/blob/main/lab/005-rare-hello-fod/containerlab-fod-freertr.sh> (requires containerlab to be installed)

"FoD in a box" based on Containerlab: Automated Mitigation Demo

- runs only in terminal, not via Web UI
- rules emitted into FoD via Python code

Demo

NeMo with freertr: installation and use

End

