Walkthrough of NeMo Integration with RARE for DDoS Attack Detection and Mitigation

Nikos Kostopoulos, NTUA/GRNET

David Schmitz, Leibniz Supercomputing Centre

Infoshare: Relying on RARE for DDoS Attack Protection

Online Infoshare

December 8th, 2023

GN5-1

NeMo DDoS Protection Software

Efficient DDoS attack detection and mitigation solution developed by DFN

Key features:

- Open-source
- NetFlow-based analysis for detecting traffic anomalies
- Low software requirements – Container support
- Privacy-preserving operation – sensitive data are analyzed locally
- Attack mitigation based on fine-grained filtering rules (BGP FlowSpec)

Goal

Integrate RARE Platform with NeMo for efficient DDoS detection and mitigation

- **Ongoing effort started in GN5-1**
- **The RARE team strongly collaborates with NeMo engineers**
- **GN5-1 Y1 outcome:** The RARE Platform can support mitigation rules installed by NeMo components
- **This presentation:** Proof-of-concept of RARE/NeMo integration

Components of the Setup

The DDoS protection setup consists of 4 components:

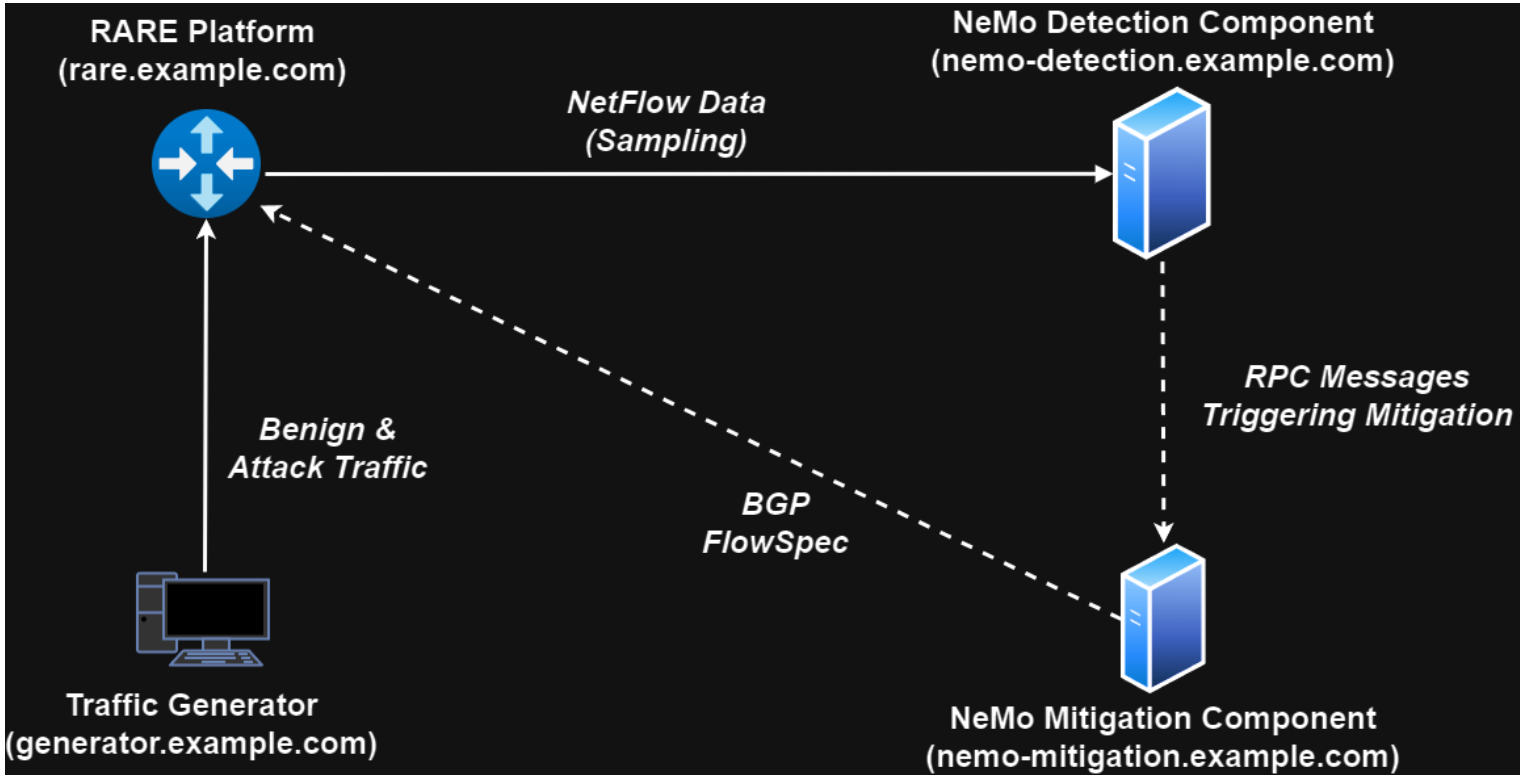
- **Traffic Generator:** Forwards traffic to the attack victim through the RARE Platform
- **RARE Platform:** Routing platform exporting monitoring data and filtering traffic
- **NeMo Detection Component:** NeMo software that detects ongoing attacks and triggers attack mitigation requests
- **NeMo Mitigation Component:** NeMo software that installs mitigation rules to the RARE Platform

Setup Specifications

Our experimental testbed involved 4 VM's with the following specifications:

Component	DNS Name	Hardware Specifications
Traffic Generator	*generator.example.com*	2 cores, 2 GB RAM
RARE Platform	*rare.example.com*	2 cores, 4 GB RAM
NeMo Detection Component	*nemo-detection.example.com*	2 cores, 8 GB RAM
NeMo Mitigation Component	*nemo-mitigation.example.com*	4 cores, 8 GB RAM

High-Level Overview of the Setup



- DDoS attack detection relies on **NetFlow data** sampled from the RARE Platform (**FreeRtr** routing software)
- The NeMo Detection Component submits **mitigation requests** to the NeMo Mitigation Component via **RPC messages**
- Mitigation rules are installed at the RARE Platform via **BGP FlowSpec**

Traffic Generator – Implementation Details

Purpose: Forwards benign and attack traffic to the RARE Platform

Traffic may be:

- Available from production traffic and replayed with **Tcpreplay** at specified rates
- Synthetically generated based on multiple software solutions
  - hping3
  - Python Scapy
  - Mausezahn

RARE Platform – Implementation Details

Purpose:

- Routing software - FreeRtr
- Export of NetFlow-based monitoring data
- Installation of malicious traffic filtering rules by NeMo components

Configuration:

- IP address configuration for router interfaces
- NetFlow configuration to receive sampled monitoring data
- BGP FlowSpec support for mitigation rule installation

NeMo Detection Component – Implementation Details

Purpose:

- NeMo User Interface (UI)
- Definition of anomaly detection rules and detection of ongoing attacks (e.g. by detecting violations of predefined thresholds)
- Triggering installation of appropriate mitigation rules

NeMo Software Installation:

- Automated script for parameter configuration
- Docker containerization

NeMo Detection Component – Implementation Details

Purpose:

- Installation of mitigation rules to the RARE Platform
- Collection of statistics from RARE to monitor the attack mitigation process

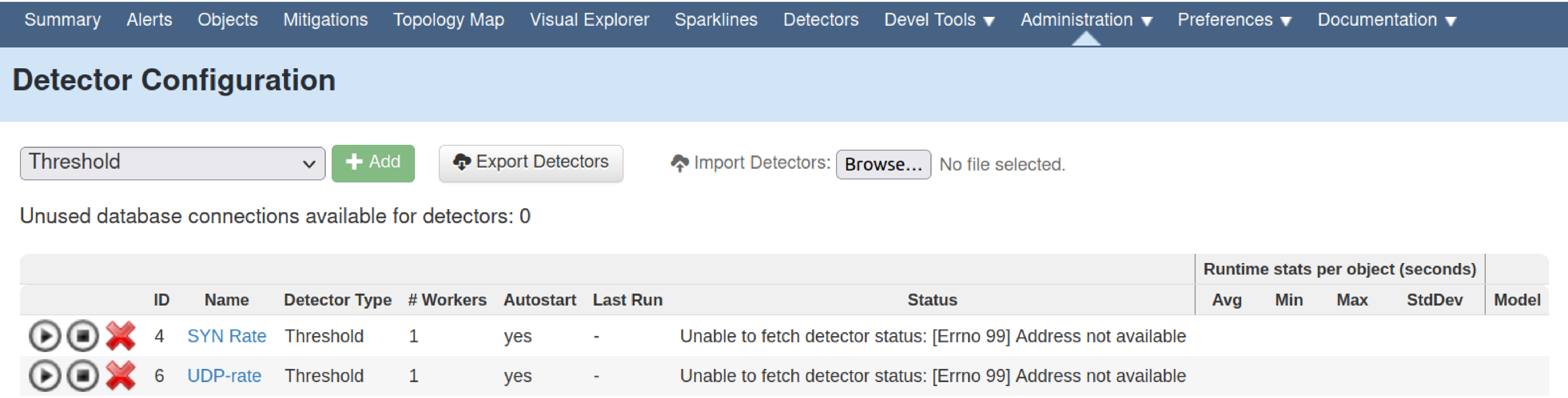
Configuration:

- NeMo parameters for RPC communication between the NeMo Detection and Mitigation Components
- BGP speaker configuration – **ExaBGP**
- Python script for collecting **FlowSpec** statistics from FreeRtr

Proof-of-Concept

DDoS Protection Walkthrough

Detector Configuration



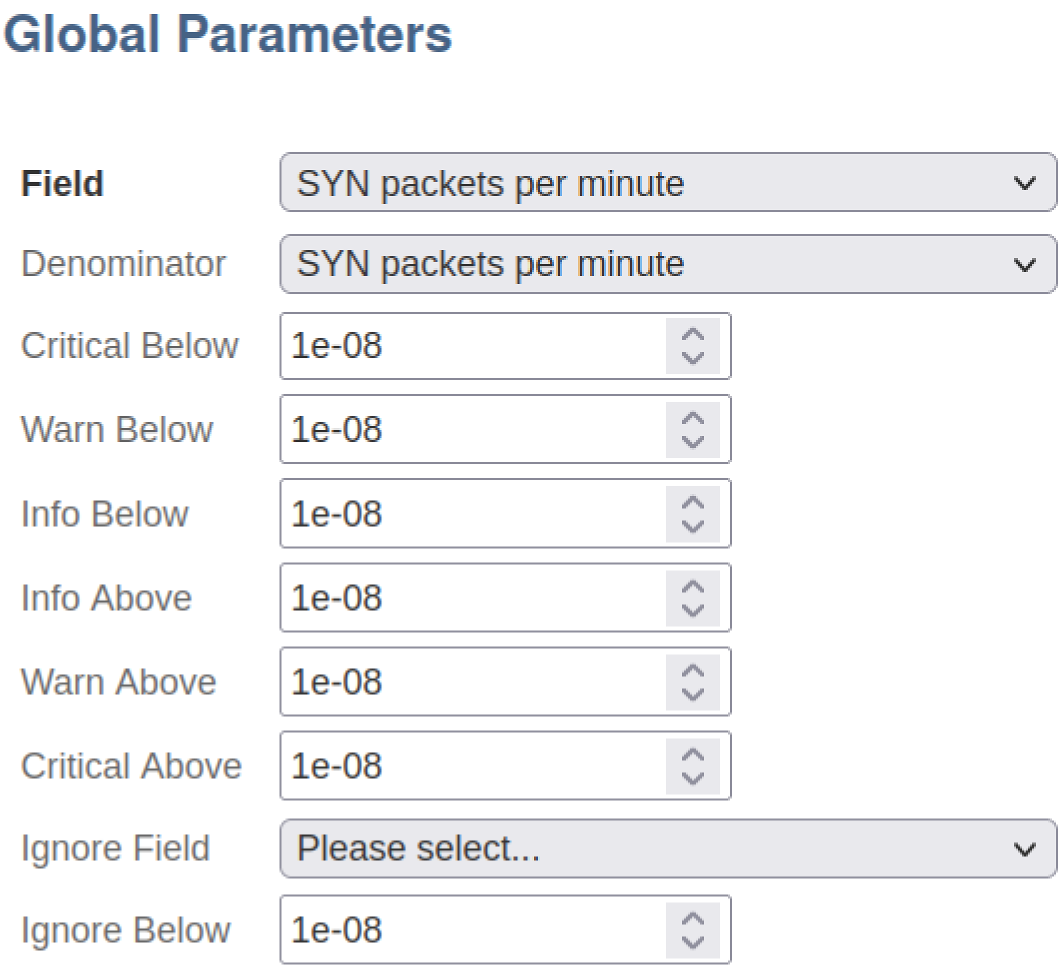
Detector Configuration

Unused database connections available for detectors: 0

								Runtime stats per object (seconds)				
	ID	Name	Detector Type	# Workers	Autostart	Last Run	Status	Avg	Min	Max	StdDev	Model
▶ ■ ✖	4	SYN Rate	Threshold	1	yes	-	Unable to fetch detector status: [Errno 99] Address not available					
▶ ■ ✖	6	UDP-rate	Threshold	1	yes	-	Unable to fetch detector status: [Errno 99] Address not available					

The 1st step requires configuring **detectors**, e.g. **threshold-based rules** for detecting violations pertaining to specific traffic categories

Threshold Detectors – Settings Parameters

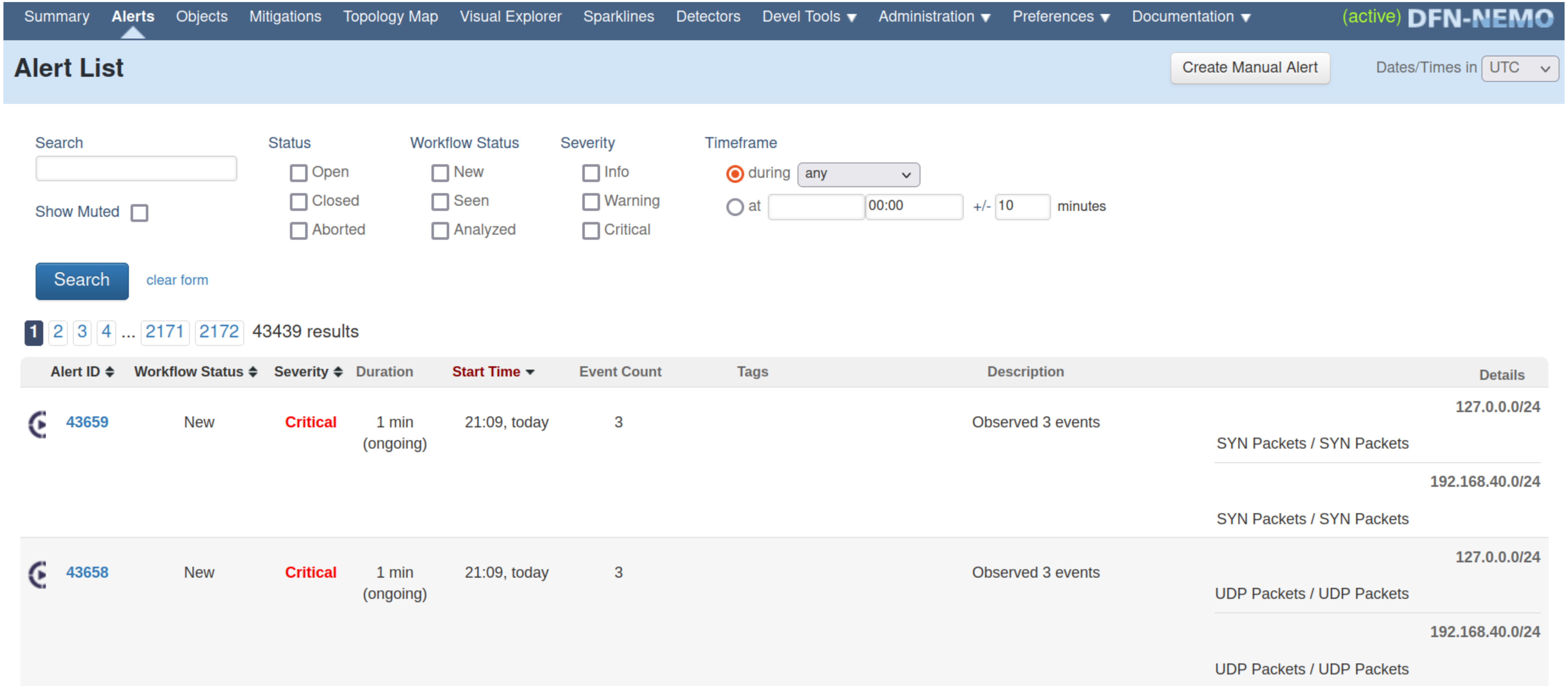


Global Parameters

Field	SYN packets per minute
Denominator	SYN packets per minute
Critical Below	1e-08
Warn Below	1e-08
Info Below	1e-08
Info Above	1e-08
Warn Above	1e-08
Critical Above	1e-08
Ignore Field	Please select...
Ignore Below	1e-08

Multiple **threshold levels** (warning level, critical level, …) may be defined by the administrator

NeMo Alerts



Alert List

Dates/Times in UTC

Search

Show Muted □

Status: □ Open □ Closed □ Aborted

Workflow Status: □ New □ Seen □ Analyzed

Severity: □ Info □ Warning □ Critical

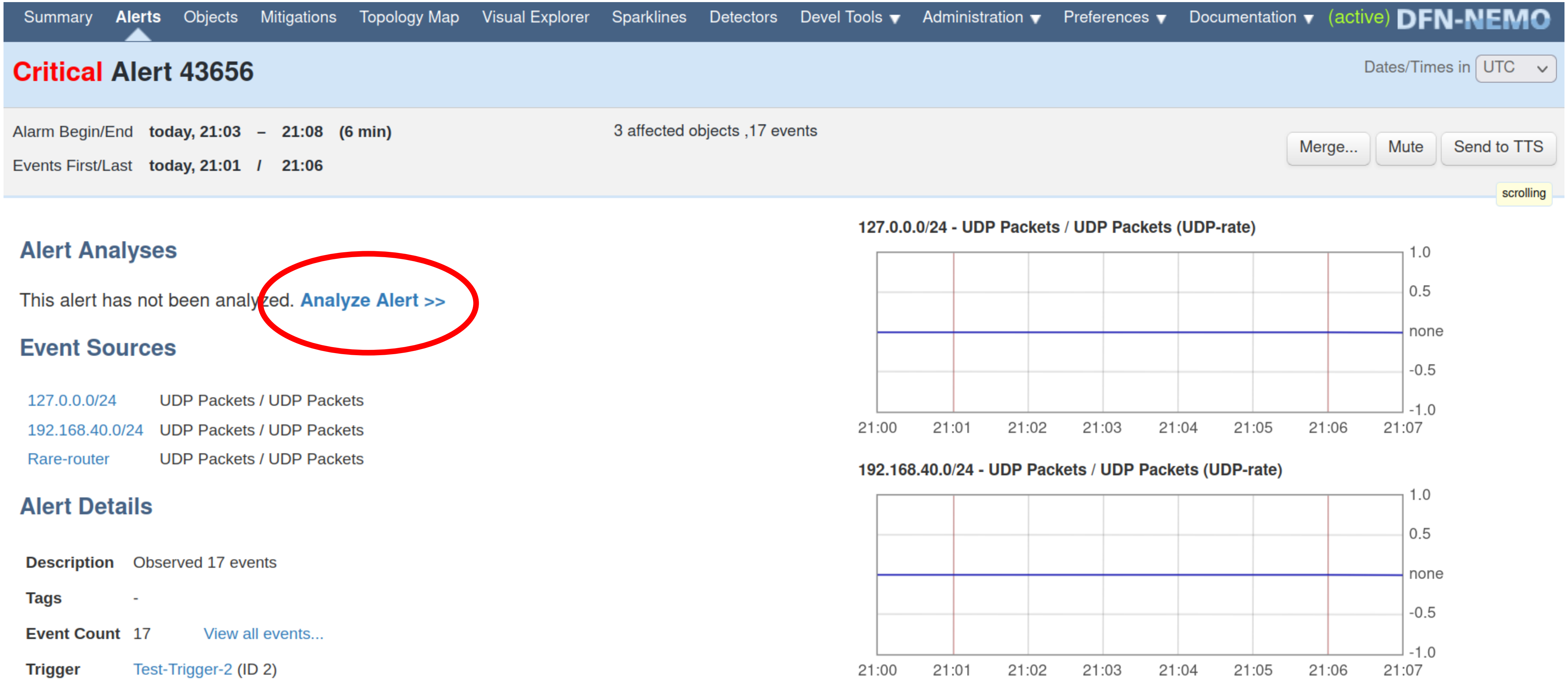
Timeframe: ● during any
○ at 00:00 +/- 10 minutes

1 2 3 4 ... 2171 2172 43439 results

Alert ID	Workflow Status	Severity	Duration	Start Time	Event Count	Tags	Description	Details
43659	New	Critical	1 min (ongoing)	21:09, today	3		Observed 3 events	127.0.0.0/24 SYN Packets / SYN Packets 192.168.40.0/24 SYN Packets / SYN Packets
43658	New	Critical	1 min (ongoing)	21:09, today	3		Observed 3 events	127.0.0.0/24 UDP Packets / UDP Packets 192.168.40.0/24 UDP Packets / UDP Packets

Alerts raised by NeMo based on the defined detectors

NeMo Alerts - Analysis



Critical Alert 43656

Alarm Begin/End today, 21:03 – 21:08 (6 min)

Events First/Last today, 21:01 / 21:06

3 affected objects ,17 events

Alert Analyses

This alert has not been analyzed. Analyze Alert >>

Event Sources

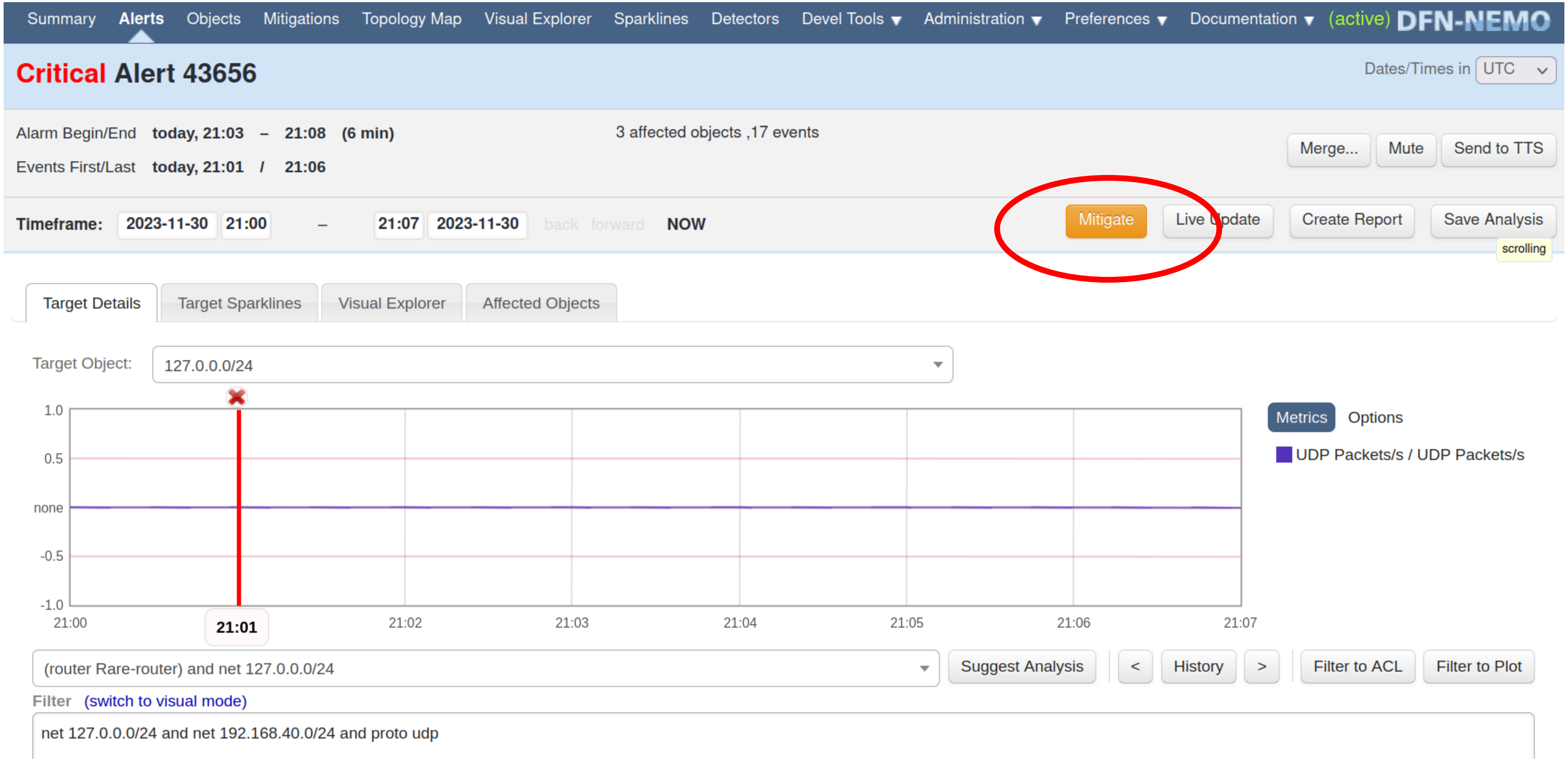
127.0.0.0/24	UDP Packets / UDP Packets
192.168.40.0/24	UDP Packets / UDP Packets
Rare-router	UDP Packets / UDP Packets

Alert Details

Description	Observed 17 events
Tags	-
Event Count	17 View all events...
Trigger	Test-Trigger-2 (ID 2)

Administrators may further **analyze** the raised alerts to delve into their characteristics

NeMo Alerts – Triggering Mitigation



Critical Alert 43656

Dates/Times in UTC

Alarm Begin/End today, 21:03 – 21:08 (6 min)

Events First/Last today, 21:01 / 21:06

3 affected objects ,17 events

Timeframe: 2023-11-30 21:00 – 21:07 2023-11-30

Target Object: 127.0.0.0/24

■ UDP Packets/s / UDP Packets/s

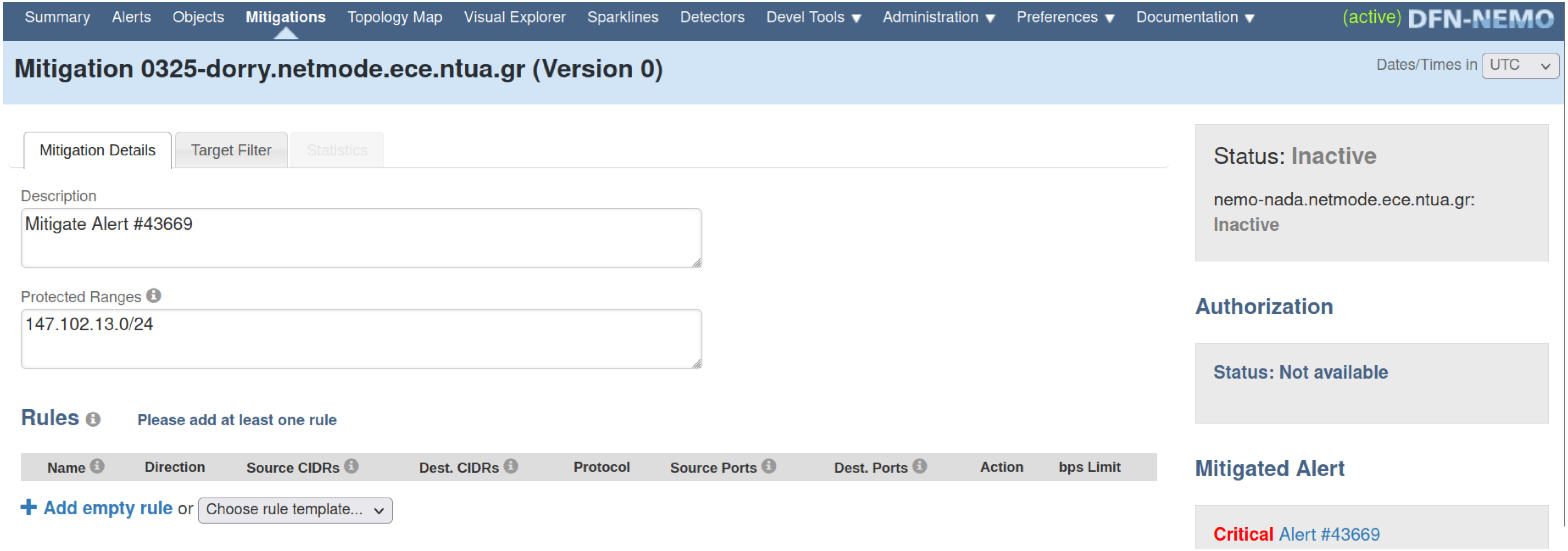
(router Rare-router) and net 127.0.0.0/24

Filter

net 127.0.0.0/24 and net 192.168.40.0/24 and proto udp

After analyzing the characteristics of the detected anomalies, Administrators may trigger the installation of attack mitigation rules

NeMo Alerts – Mitigation (1/6)



Mitigation 0325-dorry.netmode.ece.ntua.gr (Version 0)

Dates/Times in UTC

Description: Mitigate Alert #43669

Protected Ranges: 147.102.13.0/24

Rules

Please add at least one rule

Name	Direction	Source CIDRs	Dest. CIDRs	Protocol	Source Ports	Dest. Ports	Action	bps Limit

+ Add empty rule or Choose rule template...

Status: Inactive

nemo-nada.netmode.ece.ntua.gr: Inactive

Authorization

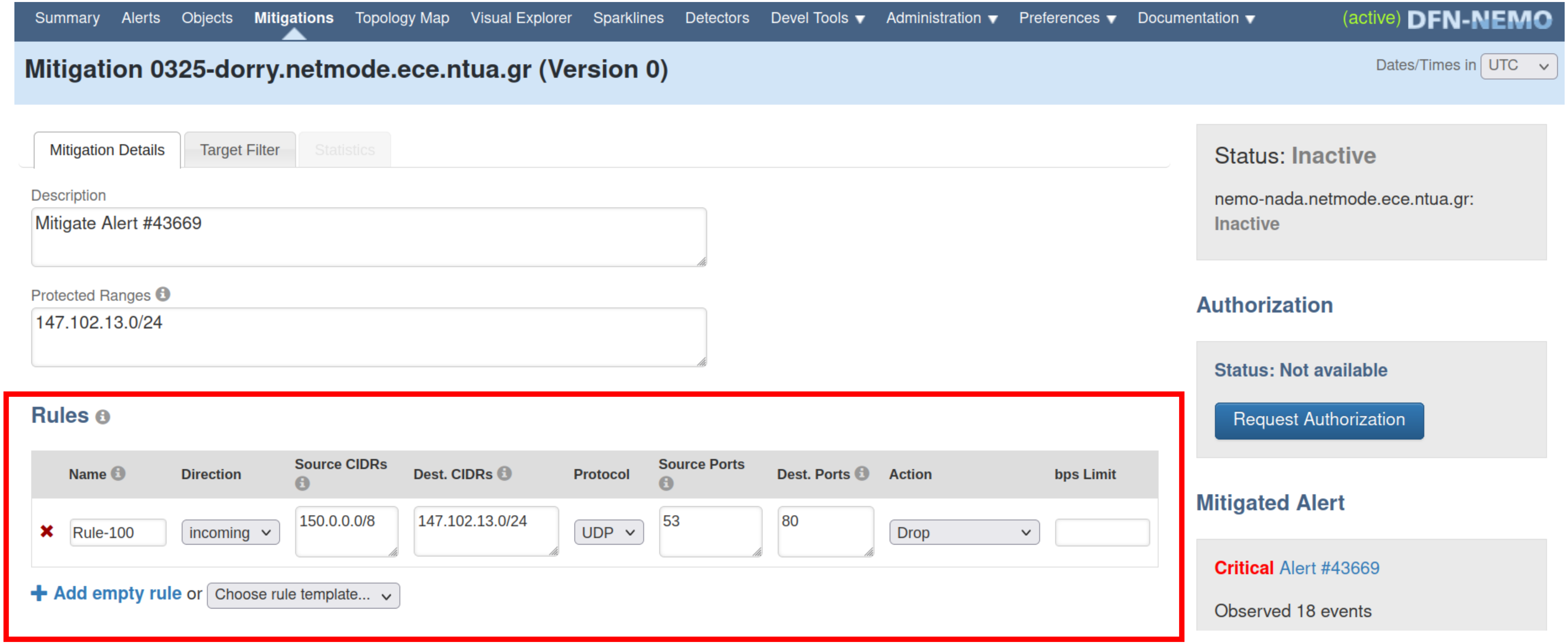
Status: Not available

Mitigated Alert

Critical Alert #43669

Administrators define the protected ranges

NeMo Alerts – Mitigation (2/6)



Mitigation 0325-dorry.netmode.ece.ntua.gr (Version 0)

Description: Mitigate Alert #43669

Protected Ranges: 147.102.13.0/24

Rules

	Name	Direction	Source CIDRs	Dest. CIDRs	Protocol	Source Ports	Dest. Ports	Action	bps Limit
✖	Rule-100	incoming	150.0.0.0/8	147.102.13.0/24	UDP	53	80	Drop	

Status: Inactive

nemo-nada.netmode.ece.ntua.gr: Inactive

Authorization

Status: Not available

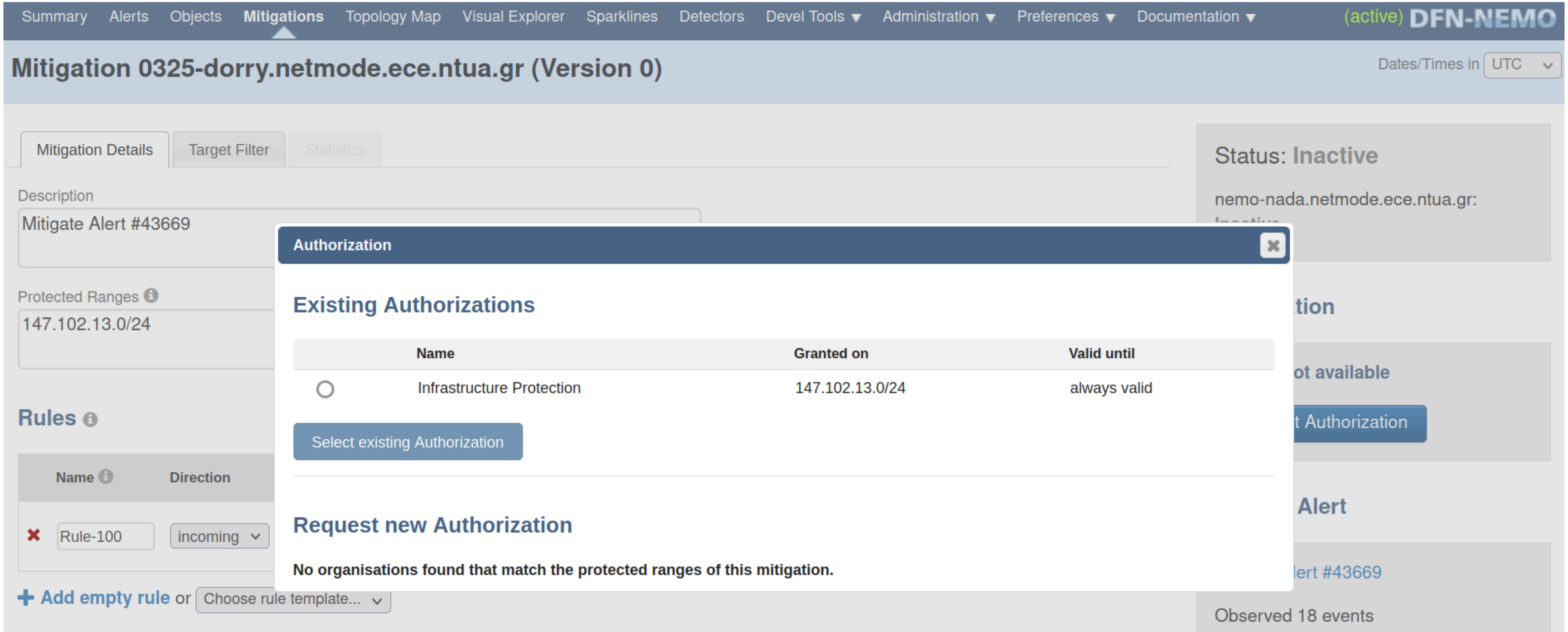
Mitigated Alert

Critical Alert #43669

Observed 18 events

Administrators may define mitigation details

NeMo Alerts – Mitigation (3/6)



Mitigation 0325-dorry.netmode.ece.ntua.gr (Version 0)

Dates/Times in UTC

Description: Mitigate Alert #43669

Protected Ranges: 147.102.13.0/24

Rules

	Name	Direction
✖	Rule-100	incoming

Status: Inactive

nemo-nada.netmode.ece.ntua.gr:

Authorization

Existing Authorizations

	Name	Granted on	Valid until
○	Infrastructure Protection	147.102.13.0/24	always valid

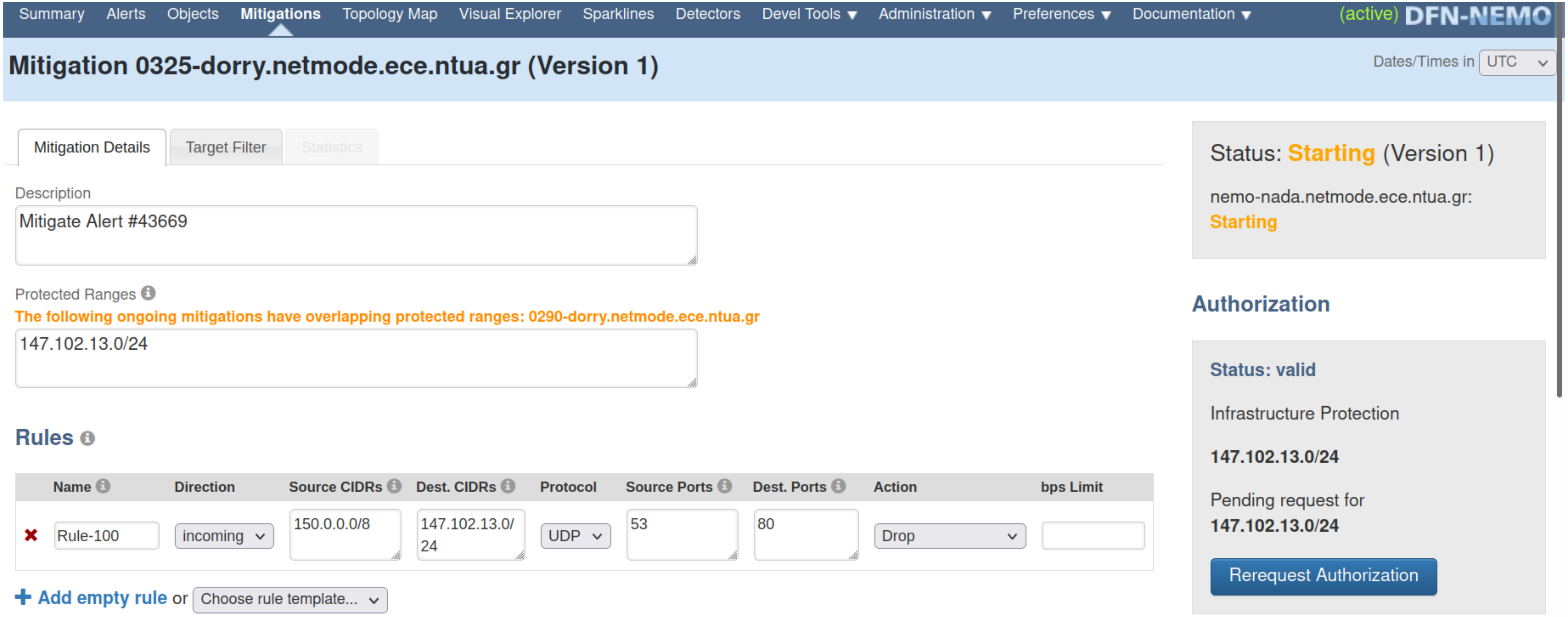
Request new Authorization

No organisations found that match the protected ranges of this mitigation.

Observed 18 events

Authorization is required before triggering the installation of mitigation rules

NeMo Alerts – Mitigation (4/6)



Mitigation 0325-dorry.netmode.ece.ntua.gr (Version 1)

Dates/Times in UTC

Description: Mitigate Alert #43669

Protected Ranges

The following ongoing mitigations have overlapping protected ranges: 0290-dorry.netmode.ece.ntua.gr

147.102.13.0/24

Rules

	Name	Direction	Source CIDRs	Dest. CIDRs	Protocol	Source Ports	Dest. Ports	Action	bps Limit
✖	Rule-100	incoming	150.0.0.0/8	147.102.13.0/24	UDP	53	80	Drop	

Status: Starting (Version 1)

nemo-nada.netmode.ece.ntua.gr: Starting

Authorization

Status: valid

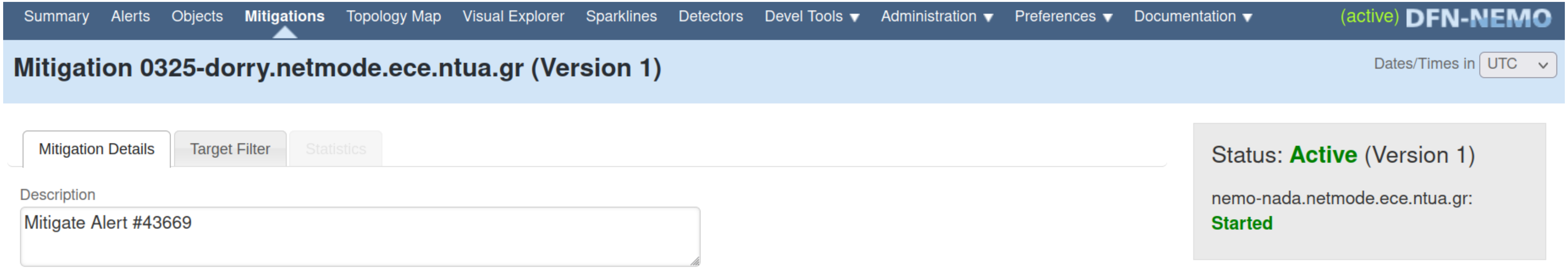
Infrastructure Protection

147.102.13.0/24

Pending request for 147.102.13.0/24

The mitigation process starts

NeMo Alerts – Mitigation (5/6)



Mitigation 0325-dorry.netmode.ece.ntua.gr (Version 1)

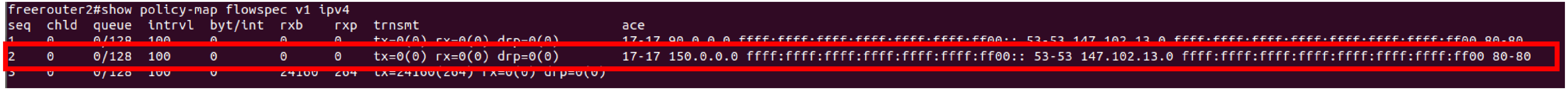
Description
Mitigate Alert #43669

Status: Active (Version 1)

nemo-nada.netmode.ece.ntua.gr: Started

Status: **Active** → Mitigation rules have been installed at the RARE Platform

NeMo Alerts – Mitigation (6/6)



```
freerouter2#show policy-map flowspec v1 ipv4
seq  chld   queue  intrvl  byt/int  rxb     rxp  trnsmt                          ace
1    0      0/128  100     0        0       0    tx=0(0) rx=0(0) drp=0(0)        17-17 90.0.0.0 ffff:ffff:ffff:ffff:ffff:ffff:ff00:: 53-53 147.102.13.0 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 80-80
2    0      0/128  100     0        0       0    tx=0(0) rx=0(0) drp=0(0)        17-17 150.0.0.0 ffff:ffff:ffff:ffff:ffff:ffff:ff00:: 53-53 147.102.13.0 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 80-80
3    0      0/128  100     0        24160   264  tx=24160(264) rx=0(0) drp=0(0)
```

Output of “**show policy-map flowspec VRF ipv4**” command that shows **flowspec-related** rules at FreeRtr

Future Steps

- Automation of the DDoS protection setup within **Containerlab**
- Evaluation of the DDoS protection setup based on production data
- Stress testing to evaluate DDoS attack filtering throughput
- Experimentation with the diverse NeMo attack detection methods

Thank You

Homepage: https://wiki.geant.org/display/RARE/Home

RARE Developers Mailing List: rare-dev@lists.geant.org

Co-funded by
the European Union