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

<table>
<thead>
<tr>
<th>Component</th>
<th>DNS Name</th>
<th>Hardware Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Generator</td>
<td>generator.example.com</td>
<td>2 cores, 2 GB RAM</td>
</tr>
<tr>
<td>RARE Platform</td>
<td>rare.example.com</td>
<td>2 cores, 4 GB RAM</td>
</tr>
<tr>
<td>NeMo Detection Component</td>
<td>nemo-detection.example.com</td>
<td>2 cores, 8 GB RAM</td>
</tr>
<tr>
<td>NeMo Mitigation Component</td>
<td>nemo-mitigation.example.com</td>
<td>4 cores, 8 GB RAM</td>
</tr>
</tbody>
</table>
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**
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
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
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
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
DDoS Protection Walkthrough
The 1st step requires configuring detectors, e.g. threshold-based rules for detecting violations pertaining to specific traffic categories.
Multiple **threshold levels** (warning level, critical level, ...) may be defined by the administrator.
Alerts raised by NeMo based on the defined detectors
Administrators may further analyze the raised alerts to delve into their characteristics.
After analyzing the characteristics of the detected anomalies, Administrators may trigger the installation of attack mitigation rules.
Administrators define the protected ranges
Administrators may define mitigation details
Authorization is required before triggering the installation of mitigation rules
The mitigation process starts
Status: Active ➔ Mitigation rules have been installed at the RARE Platform
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