DDoS Attack Mitigation with Firewall on Demand (FoD) and RARE

Nikos Kostopoulos, National Technical University of Athens (Greece)
David Schmitz, Leibniz Supercomputing Centre (Germany)

TNC24, Rennes, France

12 June 2024

Demo Overview

A use case of Distributed Denial of Service (DDoS) attack mitigation based on **GÉANT open-source software solutions:**

- **RARE:** Router for Academia, Research & Education
- **FoD:** Firewall on Demand

RARE:

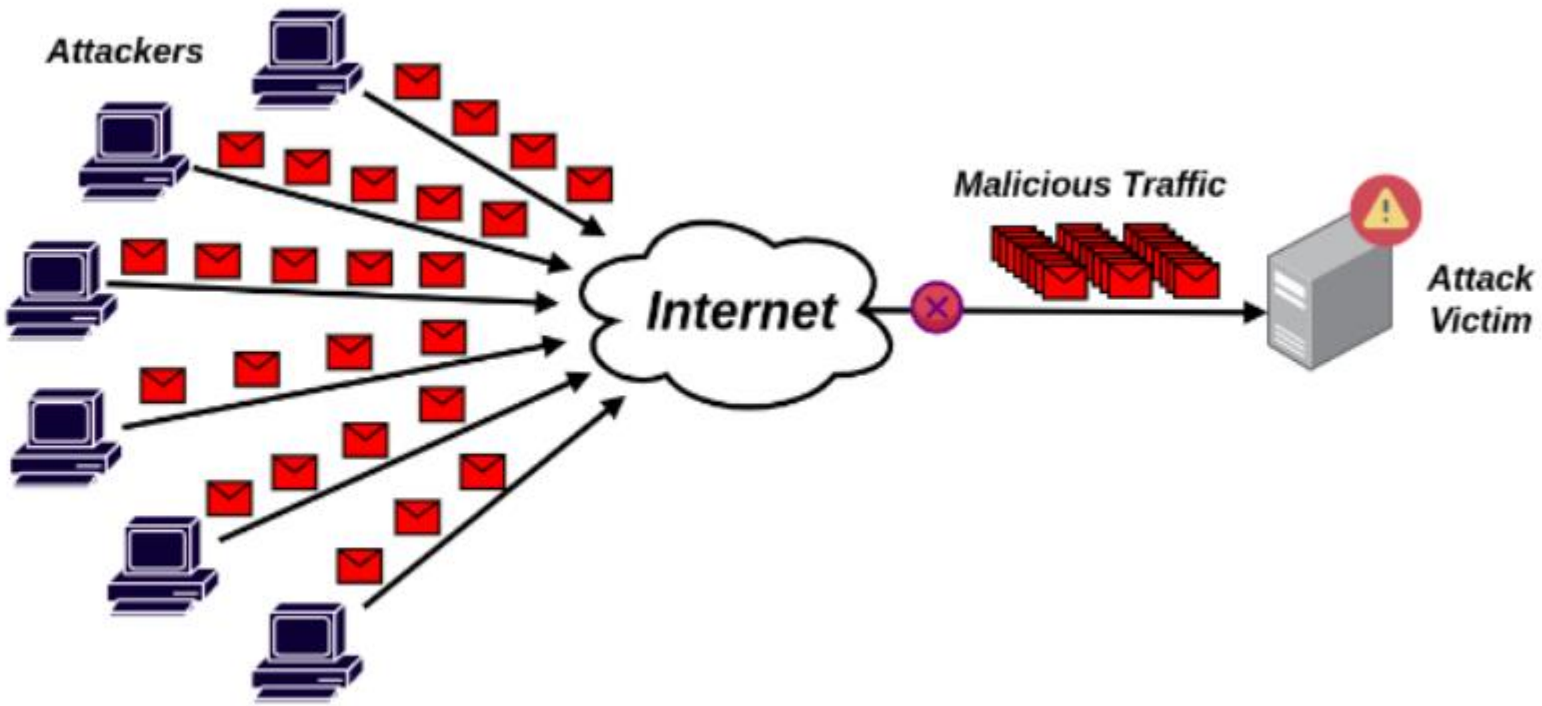
- Solutions for Research & Education (R&E) use cases based on routing software platforms
- Developed under GN5-1, Work Package 6

FoD:

- System and GÉANT service for effective DDoS attack mitigation
- Developed under GN5-1, Work Package 8

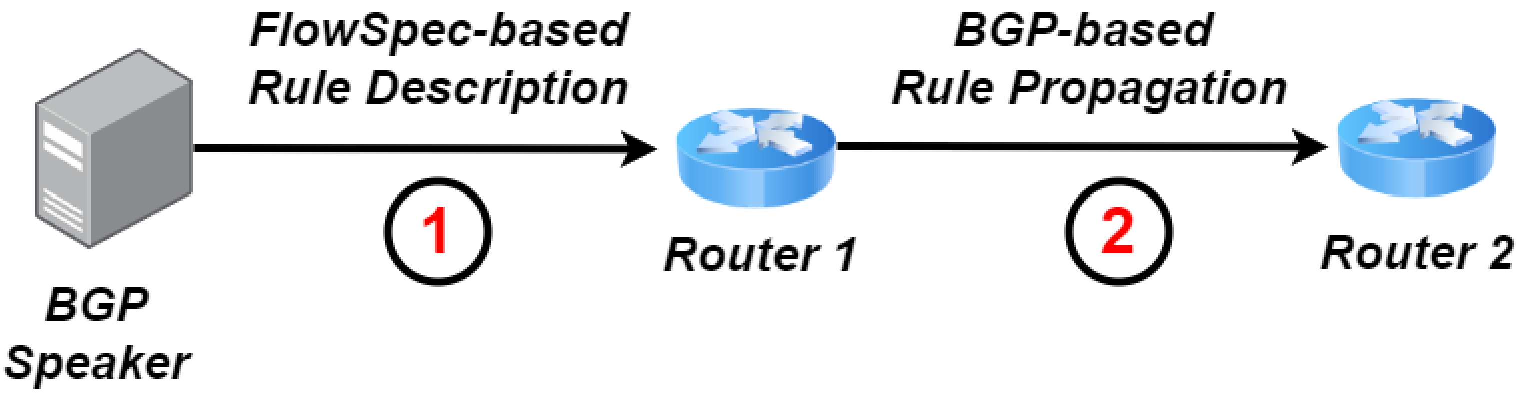
Background: DDoS Attacks

- Multiple Internet sources (e.g. Internet of Things – IoT devices) flood victims with massive traffic to deplete:
  - System resources (e.g. processors and/or memory)
  - Bandwidth of links leading to victims
- Victims are unable to process legitimate traffic, which is eventually discarded



Background: FlowSpec-based DDoS Attack Mitigation

- **Flow Specification (FlowSpec)** matches traffic based on flow characteristics that may involve:
  - source/destination IP addresses
  - source/destination port numbers
  - protocol types (e.g. TCP, UDP, ICMP)
- Matched traffic may be dropped, rate limited or redirected for further inspection
- **Border Gateway Protocol (BGP)** enables the propagation of FlowSpec rules to upstream routers, thus facilitating distributed DDoS attack mitigation
- FlowSpec rules are usually triggered by a **BGP Speaker** (e.g. ExaBGP)

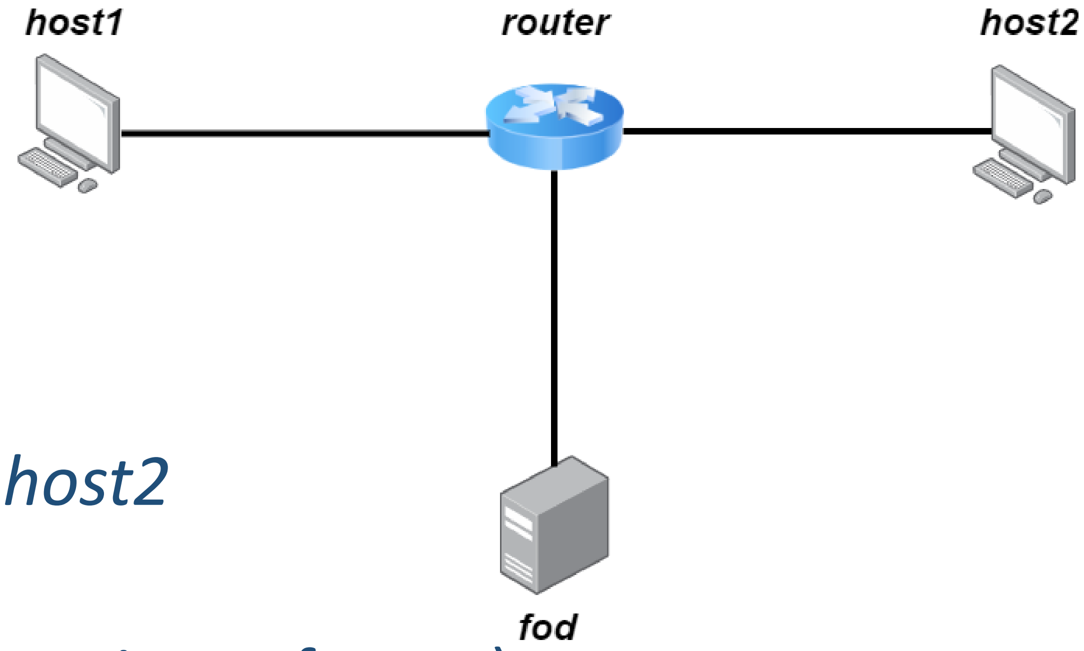


Firewall on Demand – FoD

FoD relies on BGP FlowSpec for DDoS attack mitigation

- **FoD characteristics:**
  - Mitigation actions are triggered by users themselves
    → Users may start, edit and stop the mitigation process
  - Multi-tenant, eduGAIN-based
  - Involves both a User Interface (UI) and a REST API
  - Based on the ExaBGP BGP speaker to establish neighborships with routers and trigger DDoS attack mitigation
- **GÉANT FoD service instance:**
  - Enables mitigation within the GÉANT core
  - NREN NOC admins trigger mitigation actions without contacting GÉANT NOC
  - Productive for more than 8 years

Demo Setup



Components:

- ***host1***: Simulates an ICMP flood attack against *host2*
- ***host2***: The attack victim
- ***router***: RARE platform (relying on the ***freeRtr*** routing software)
  - → Forwards network traffic
  - → Exports NetFlow data to the FoD platform for further analysis
  - → Filters traffic based on BGP FlowSpec
- ***fod***: The Firewall on Demand (FoD) platform
  - → Analyzes the received NetFlow records
  - → Triggers DDoS attack mitigation

Automated Setup based on Containerlab

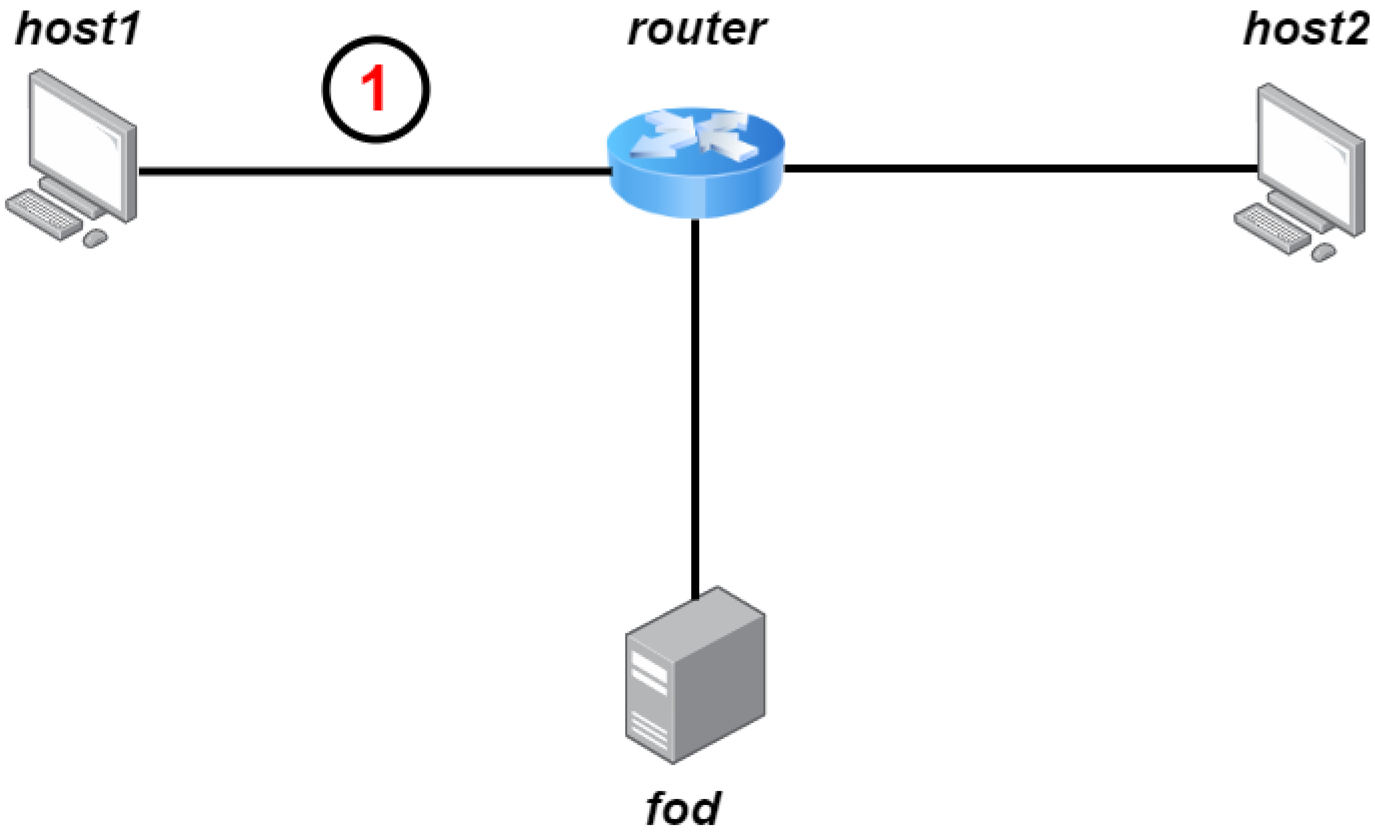
- The demo setup is automated based on **Docker** and **Containerlab**

Containerlab:

- Includes Command Line Interface (CLI) tools for creating and managing container-based networking labs
- Handles the networking between the containers of the lab topology

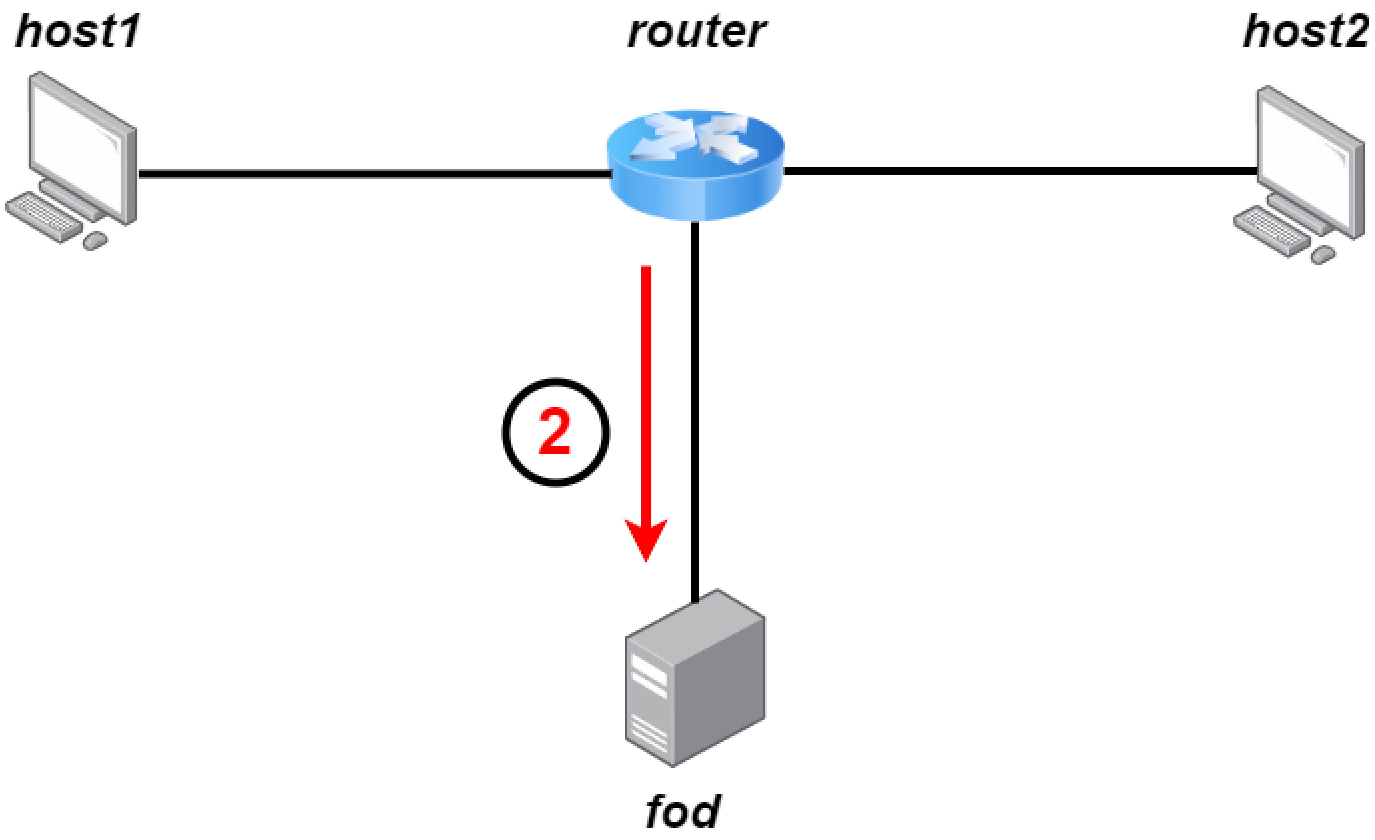
→ *topology.clan.yml*: Contains general information about the lab and involves details about the container networking

Demo Process (1/5)



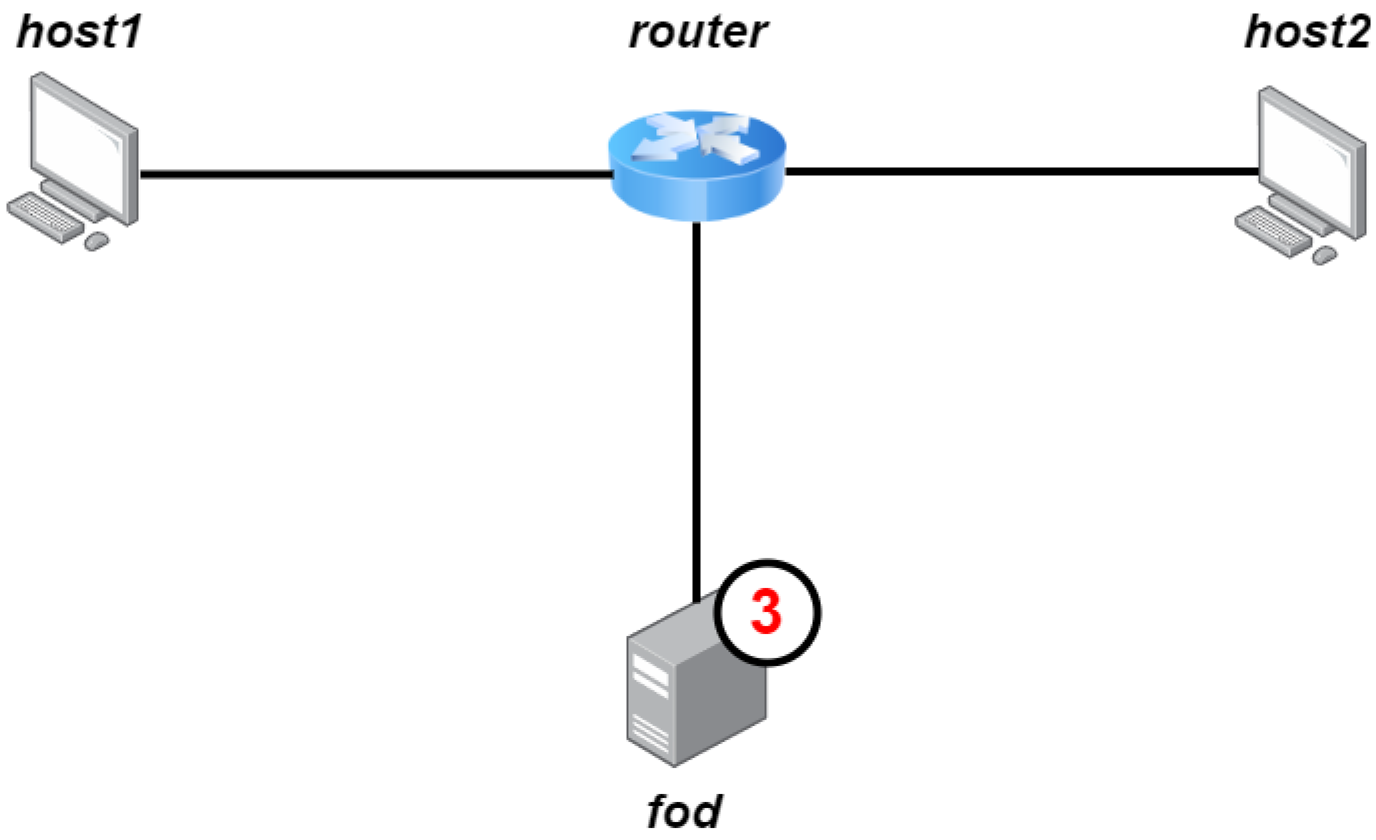
An **ICMP flood attack** will be executed from *host1* against *host2* using the **hping3** traffic simulator

Demo Process (2/5)



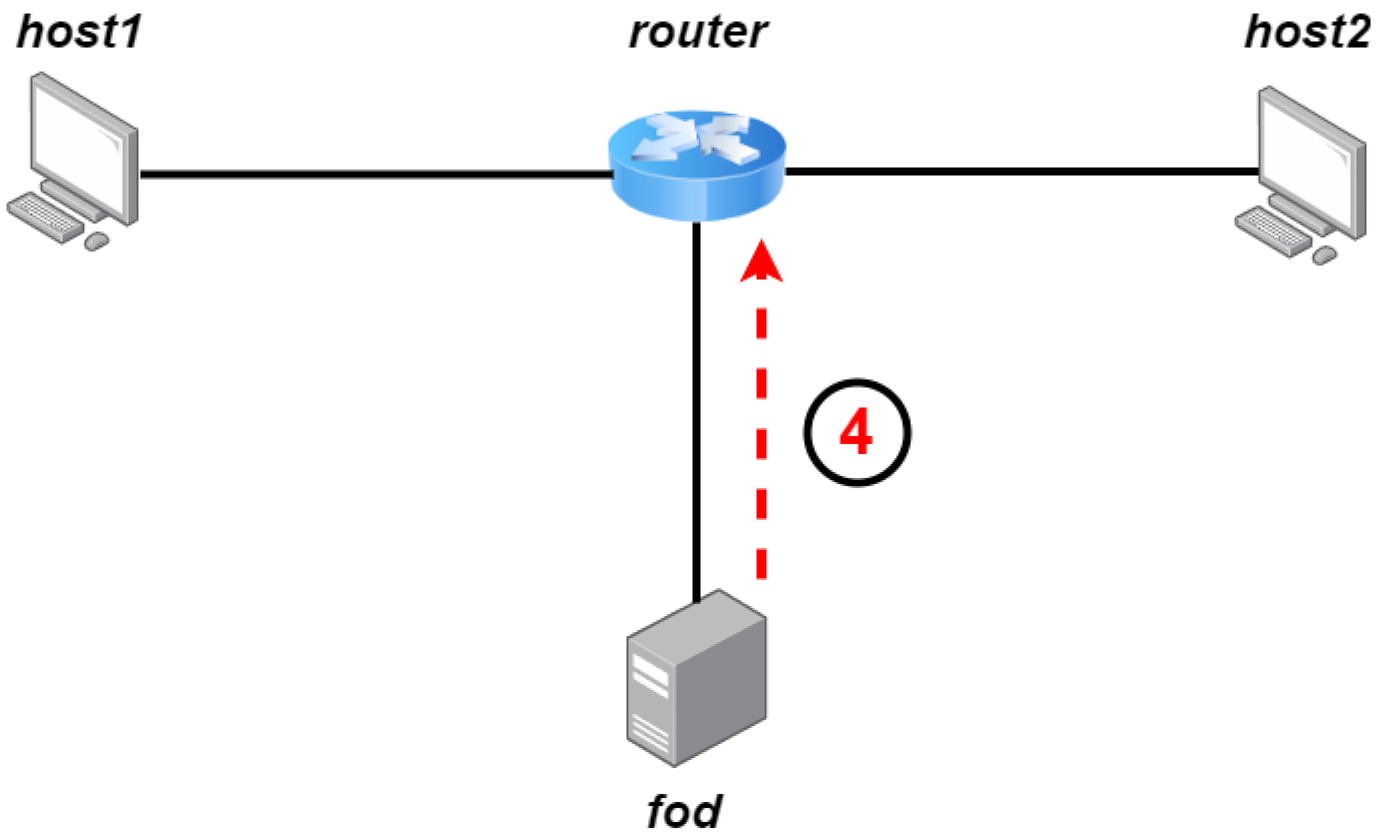
NetFlow records will be exported from the *router* to the *fod*

Demo Process (3/5)



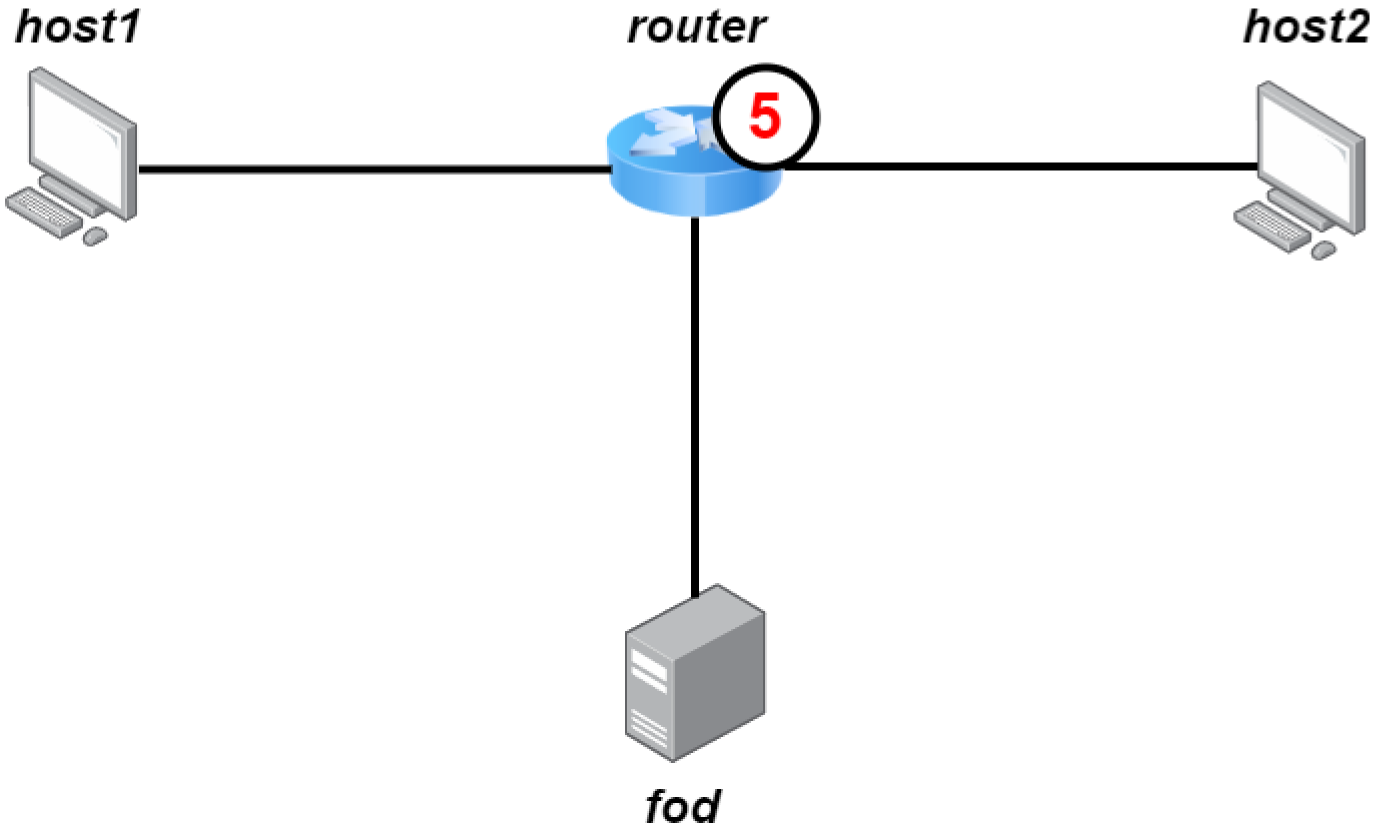
NetFlow data will be analyzed to detect an **ongoing attack** and determine the appropriate **filtering rules** (based on the attacker source IP)

Demo Process (4/5)



The **ExaBGP BGP speaker** will install appropriate mitigation rules to the *router* based on **BGP FlowSpec**

Demo Process (5/5)



Malicious traffic from the attacker IP will be dropped at the *router*

How to Replicate

1) Clone the demo repository:

→ *git clone https://github.com/nkostopoulos/rare-fod*

2) Deploy the Containerlab topology:

→ *containerlab deploy --topo topology.clab.yml*

3) Execute the appropriate commands to configure the Docker containers:

→ *python3 setup.py*

4) Verify that mitigation takes place by inspecting the "ifconfig" statistics for hosts *host1* and *host2*

Thank You

RARE mailing list: gn5-1-wp6-t1-rare@lists.geant.org

www.geant.org

Co-funded by
the European Union