AUTOMATION OF DDOS ATTACK MITIGATION

BRNO UNIVERSITY OF TECHNOLOGY

AUTHOR: Ing. Peter Nagy SUPERVISOR: Ing. Matěj Grégr, Ph.D.

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Introduction

DDoS attacks are a rapidly growing problem. Attacks are getting bigger and more complex. To solve this issue, we developed an automation system for DDoS attack mitigation by utilizing BGP Flowspec standard, REST API and opensource detection tools. Automation of DDoS attack mitigation was integrated to the NETX platform.

Platform overview

NETX is an open source routing platform used for high-performance open source routing developed at the Brno University of Technology. Thanks to rich experience in high performance networking, this product provides a massive set of routing features as well as traffic shaping capabilities. It can handle several full BGP tables and supports a lot of other networking protocols. NETX was selected as open source target platform according to:

A. Hardware filtration – offloading packet filtration ACLs to NIC.
B. Easy to use modular system with CLI and API.
C. High performance, usable for bigger networks.

Netc

Netc was created to simplify the router configuration using Cisco-like commands to make the whole system configurable on one place.

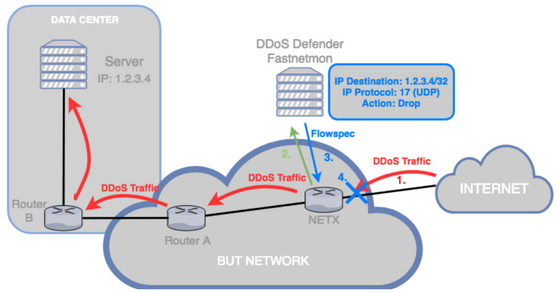

Figure A: BGP Flowspec real-world architecture.

Detection tools

The following DDoS detection tools were evaluated and integrated to the automation system:

Selected DDoS Defection tools

- **DDoS Defender**
- **FastNetMon**

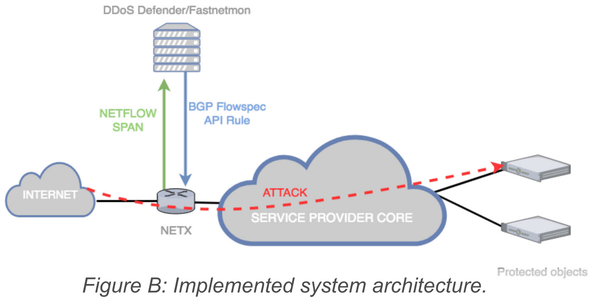

Figure B: Implemented system architecture.

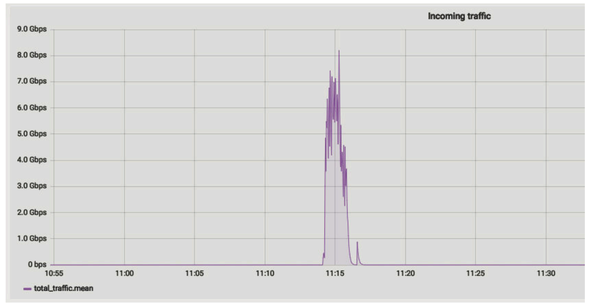

Figure C: DDoS Attack Mitigation

Attack mitigation

One of the primary objective of the mitigation is to stop only the DDoS attacks and not regular traffic. Detection tools detect the attack and run a custom script which gets essential information about the attack like top N source attacker IP addresses. The script sends this information to NETX using API or via BGP Flowspec as shown in Figure B. The Netc module ensures that hardware filtering is enabled and filters are correctly added.

Figure C shows ongoing DDoS attack and its automatic mitigation using FastNetMon.

The whole attack mitigation testing was done in Brno University of Technology (BUT) testing network.

Hardware filtration

To gain maximal performance and not overload the router, hardware filtration can be used. It can be described as ACLs for network card not consuming any system resources.

Those cards have an Intel Ethernet Flow Director (Intel Ethernet FD), which is mainly designed to direct the packets to the operating system core, where the consuming process or container is running

Using Intel Ethernet FD, packet processing can be offloaded to the network interface card, hence it can be used for mitigation of DDoS attacks.

Conclusion

Automated DDoS Mitigation system using NETX platform was implemented. DDoS Defender, Fastnetmon can be used as DDoS attack detection tools. The following items highlight the main contributions of the thesis:

- **NETX Netc hardware filtration module:** Module translating rules to ACLs and adding them to NIC.
- **Fastnetmon, DDoS Defender modules:** Scripts validating the attacks data, parsing and sending them to NETX using API or Flowspec.
- **Testing environment**