NetDefense: Scalable, Flexible, and Efficient DDoS Prevention with SDN and NFV

Guyue Liu
3rd PhD Student
The George Washington University
guyue@gwu.edu
https://www.linkedin.com/in/graceliugw

Timothy Wood
The George Washington University
timwood@gwu.edu

Abstract

Distributed denial-of-service attacks (DDoS) have been known for a long time and are still disrupting network operations everyday. As a result, companies are continuing to spend a large amount of money to buy the latest defense devices to cope with new variations of attacks. Is it possible to replace these expensive, fixed capacity hardware boxes with cheap, flexible and easy to scale software? In this paper, we aim to explore new cost-effective DDoS defense solutions with the advent of new software-defined technologies such as Software-Defined Networking (SDN) and Network Function Virtualization (NFV).

Keywords *Distributed denial-of-service attacks (DDoS), Software-Defined Networking (SDN), Network Function Virtualization (NFV)*

1. Introduction

In a first step, we are trying to understand new trends for current DDoS attacks and we observe DDos attacks are increasing in both volume and intelligence. On one hand, the scale of network layer attacks is increasing. Attackers typically employ so called amplification attacks to exhaust network resources, e.g., attackers can abuse UDP-based network protocols to launch DDoS exceeding hundreds of Gbps in traffic volume [2]. On the other hand, there is an evolution in the sophistication of application-layer attacks which are disguised as legitimate traffic and target specific services. The hybrid attacks use the combination of both which makes it difficult to distinguish an actual attack from a sudden rise in popularity for a given service due to a flash crowd [3].

To effectively defend these attacks and deal with the full end-to-end problem of DoS, we are designing and building NetDefense, a system ranging for efficiently processing packets up to managing a DoS mitigation infrastructure that spans one or more data centers. We now consider three principles that guide our design.

1. The system should be scalable and responsive to detect and mitigate attacks at different scales.
2. The system should be flexible and extensible to provide and deploy new defense mechanisms.
3. The system should be efficient and incur minimal additional traffic latency.

2. Architecture

Based on these principles, NetDefense leverages two emerging technologies to detect and mitigate DDoS attacks. The first one is NFV which can provide high performance packet processing and run network functions on commodity servers efficiently [7, 8]. The second one is SDN which can control network behavior centrally and steer flows in and across data centers flexibly [4, 6].

NetDefense control plane consists of two components:

1. NF Deployer which creates and manages network functions on demand.
2. SDN Flow Redirector which manages rules in the switches and directs flows in and out of NFs.

NetDefense data plane consists of three kinds of NFs:

1. Net-Layer Detector which checks packet header and detects layer 3 and layer 4 attack.
2. App-Layer Detector which examines packet payload and detect application layer attack.
3. Traffic-Cleaner which is used to mitigate attack based on the outputs of detectors.

3. Deployment

Figure 1 shows how NetDefense might be deployed in a scenario where a data center operator is working together with an ISP to detect and prevent attacks efficiently. Here a data center is under attack from several malicious traffic sources across a wide area network. Initially, there is only an Attack Warning component running in the data center, which uses lightweight monitoring of the network and end hosts to detect a possible attack.

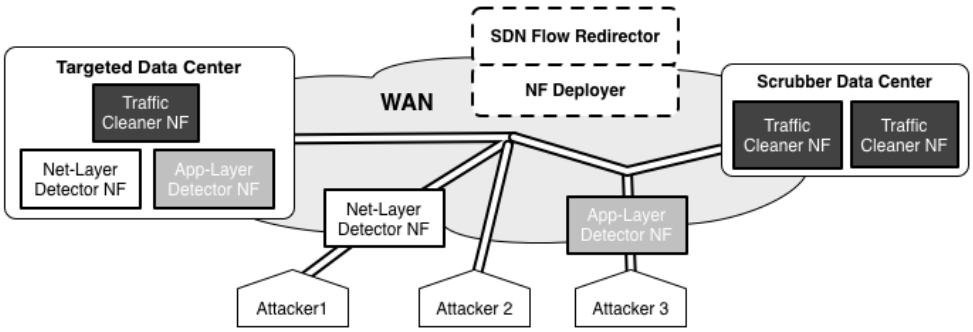

Figure 1 NetDefense deployment example

When it sees traffic rising to unusual levels, it alerts the NetDefense controller which uses the SDN Flow Redirector and the NF Deployer to instantiate a new network-layer traffic monitoring NF within the data center. This monitor incurs a minor overhead on traffic entering the data center, but it allows NetDefense to detect simple low level attacks, as well as the potential sources of the attack.

Once the network layer monitor has gathered more information about the attack, NetDefense proceeds by deploying additional monitors (potentially including application layer ones) at other data centers or middlebox locations within the ISP network. This allows NetDefense to place detection and mitigation NFs closer to the attacks. In the figure, NetDefense has also initiated mitigation NFs in a scrubber data center close to the attack sources. By redirecting traffic to that data center, attacks can be easily mitigated without causing unnecessary load on the rest of the network.

4. On-Going Work

We are implementing a prototype of our NetDefense architecture on our NetVM NFV platform [5]. We are developing efficient network monitoring NFs, including a high performance TCP Splicer NF that will allow NetDefense to very efficiently detect Layer 7 attacks. We will combine these low-level NFs with the higher level SDN framework that can efficiently redirect flows for monitoring or traffic scrubbing. There remain many exciting open questions regarding the problem of how to coordinate different kinds of NFs across data centers and how to use them for large scale traffic analysis and threat detection.

References

[1] S. Fayaz, Y. Tobioka, and V. Sekar∗ Michael Bailey. Bohatei: Flexible and Elastic DDoS Defense. in USENIX Security Symposium, 2015.

[2] C. Rossow. Amplification hell: Revisiting network protocols for ddos abuse. in USENIX Security Symposium, 2014.

[3] M. Kuhrer, T. Hupperich, C. Rossow, and T. Holz, “Exit from hell? Reducing the Impact of Amplification DDoS Attacks,” in USENIX Security Symposium, 2014.

[4] S. Jain et al. B4: Experience with a Globally-Deployed Software Defined WAN. In SIGCOMM, 2013.

[5] J. Hwang, K.K. Ramakrishnan, and T. Wood, “NetVM: high performance and flexible networking using virtualization on commodity platforms,” in Symposium on Networked System Design and Implementation, NSDI, 2014.

[6] S. Shin, V. Yegneswaran, P. Porras, and G. Gu. AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks. In Proc. CCS, 2013.

[7] T. Koponen et al. Network virtualization in multi-tenant datacenters. In Proc. NSDI, 2014.

[8] AT&T and Intel: Transforming the Network with NFV and SDN. https: //www.youtube.com/watch?v=F55pHxTeJLc#t=76.