Report: Dos/DDos defense in SDN
Spring 2014

Xinyu Tong

June 15, 2014

Contents

1 Introduction and Motivation

1.1 Definition

1.1.1 Dos/DDos

In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots (see botnet). DoS (Denial of Service) attacks are sent by one person or system.

1.1.2 SDN

Software-Defined Networking (SDN) is an emerging architecture that promises to be dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications. SDNs architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

1.2 Motivation

Now, it becomes more and more harmful to network with Dos/DDos attacks. Though we have come up with some ways to defend the attack, it for network just like what the cancer cell for body, which seems to be reasonable but leads to excessive consumption of resources. Thus, how to protect the network free of DOS has become a critical issue in current study.

2 Development of Dos/DDos defense

There are usually two ways to defend Dos/DDos attack, defense and trace-back. In this section, we mainly aim to defend the Dos/DDos attack by using a forged source IP address. Now, we will introduce three technologies in the defense of Dos/DDos.

2.1 Route-Based Packet Filter

2.1.1 Introduction

Route-based distributed packet filter determine whether a packet arriving at a router is valid with respect to its source/destination addresses, given the reach ability constraints imposed by routing and network topology.

2.1.2 Weakness

It is available only in some given situation. We use the following figure as an example. If there is Route-Based Packet Filtering in node 6, when node 7 attempts an attack to node 2 with a forged source IP address of node 4, it will be detect by node 6 because route from node 4 to node 2 won't contain the node 6. However, it will face two troubles.

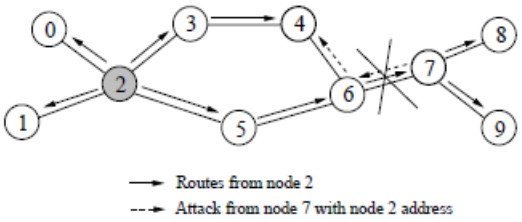

Figure 1: Route-Based Packet Filter.

1. The actual route isn't usually unique, so when one route is wrong, it will choose another route, which cause the route is difficult to determine sometimes. So, when the attacker is far away from the aim, the route is even more varied.

2. When the attacker is closed to the aim, there should be a node with Route-based distributed packet filter in the route. Thus, it sometimes need more nodes with Route-based distributed packet filter to come to a better result.

2.2 Mark the packet

2.2.1 Introduction

Then, we should come up with a new method to achieve the same aim. We notice that in the previous section, we call the filter Route-based distributed packet filter, and the way we use is to determine the routine from one node to another is logical or not. To come to the same aim, we can change the content to transmit through marking the packet.

2.2.2 Design of the mark

1. We know, the most effective way to identify whether there is a forged source IP address is to consider the first node which forwards the information. So in each node, it should add their own address in the packet to mark the routine such as the route way of DSR.

2. When the node forward the packet, it will check the packet header to determine whether the header address is directly connected to them. If there is something wrong, the node will drop the packet, otherwise, it will replace the mark header with it own address.

2.2.3 Weakness

It's essential to take the weakness into consideration in this reporter, we need to find our weakness with attacker's view. In above design, we will change the structure of the packet header, which can be change by attackers as well. That's, if I am an attacker, I can learn the network structure through constant tries. And then, knowing the structure, he can change the packet he send to escape the check. Now we must think out a method to avoid this situation, and the change of packet is also difficult to achieve.

2.3 Programmable network

As the network technology develops, Software Defined Network appears. And the achievement of the previous method becomes more easy. We may as well introduce the openflow in this section, which remote the controller and switch, makes the network an operation system.

2.3.1 Introduction

Openflow remote the switch and controller to make the network become programmable. Virtualized programmable networks could lower the bar-rier to entry for new ideas, increasing the rate of innovation in the network infrastructure.

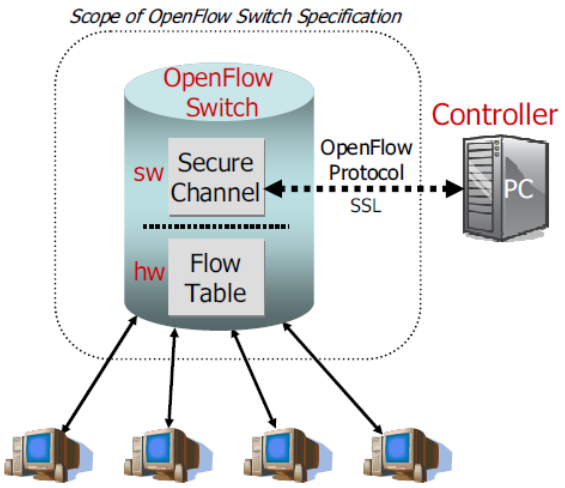

Figure 2: Idealized OpenFlow Switch.

With SDN, our goal is easier to achieve. However, the way to mark packet also has some weakness. Now, we should consider another way to achieve the same goal with different methods, which can be called flow database.

3 Network Flow Database

In openflow, we can define the network switches as the hardware in the operate system, and there are also XOR as core and API to application, etc. However, why not we use a database or cloud to share the flow information to determine whether one packet transmitted is in a logical route?

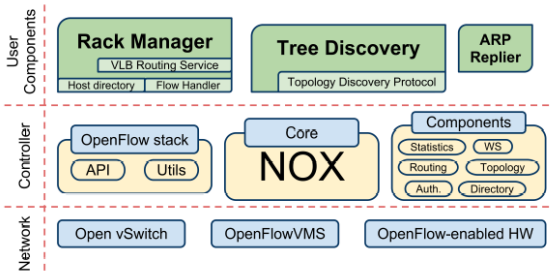

Figure 3: Component Architecture.

3.1 Introduction

Network Flow Database is somewhere to record and share the flow information, when one switch is going to forward one packet, it will register or search the information

recording the routine of packet in database. After finding the information, it will check the information to determine whether the previous node which forward the information is its own neighbor, if not, drop the packet.In order to explain how does Flow Database work, we need to explain the attack method based on reflect.

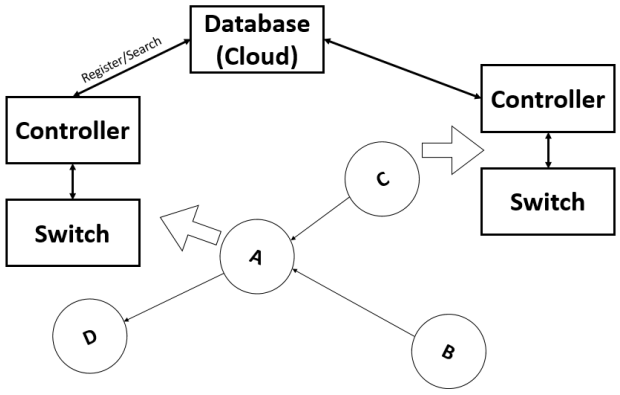

Figure 4: Structure of database.

3.1.1 Attack method

Now, let's consider the method attacker use with a forged source IP address. If node B want to attack node A by reflect, it will broad a broadcast by using node A's address. However, when the receive node response the information, they will send to node A instead of node B, which cause the consumption of node A's resource.

3.1.2 Register in database

We know it is time-consuming to search information from database, especially in a dynamic and huge database. Thus, we need a sign to make it easier to achieve this goal, that will be a key access to database.When a packet arrives, it will check whether there is a key to database, if not, meaning that this flow hasn't been recorded in database, and a random key will generate and the node will be recorded also. Then the first switch can forward the packet to the next node with the key generated.

3.1.3 Search in database

When the packet arrives, if there has been a key, it will search the information in database with the key it obtains, and when the node gets the information, it will check whether the previous node is its neighbor. If not, drop the packet.

3.1.4 Discussion

Now, we need to take the weakness into consideration. We must to attack our own study with the attacker's view. Through the study of SYN Dos attack, we know that a method seems more safe means easier to be utilized by attackers. Now, how does our database prevent being attacking?

1. When the attack want to make a broadcast with a forged source IP address, it will be always checked by the node because the "source address" is nearly never the neighbor of the first node which will forward the packet.

2. When the attack want to attack the switch through make broadcast constantly, there may be two situation happening. A. When the resource of the switch uses up, the

attacker can not send packet through this routine, which can affect the attacker in return. B. There are so many flow in database, we can limited the maximum frequency and only record the flow of broadcast. When one node generates too many broadcast information to make the switch node burst out, the node's action will be limited.