Technische Universität München
Department of Informatics

Bachelor's Thesis in Informatics

Performance analysis of Middlebox functionality

Simon Sternsdorf

Technische Universität München
Department of Informatics

Bachelor's Thesis in Informatics

Performance analysis of Middlebox functionality

Leistungsanalyse der Funktionen von Middleboxes

Author Simon Sternsdorf
Supervisor Prof. Dr.-Ing. Georg Carle
Advisor Florian Wohlfart
Date August 21, 2017

Informatik VIII
Chair for Network Architectures and Services

I confirm that this thesis is my own work and I have documented all sources and material used.

Garching b. München, August 21, 2017

Signature

Abstract

Abstract eng

Zusammenfassung

Zusammenfassung de

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Middleboxes are mediating devices used by both End-user Internet Service Providers and normal home users. The requirements ISPs have for Middleboxes are of course vastly different from the requirements of private users. Thus the implementations differs greatly as well. Middleboxes for home users do not have high performance requirements. They conduct mostly very simple tasks for a low amount of devices. This is changing of course, as more and more web-enabled devices are used in modern households. Still the required performance is low in contrast to at an ISP for example. Especially carrier grade network address translation is used to provide ipv4 connectivity for mobile phones, since IPv4 addresses are getting rare [1]. The middleboxes used are mostly implemented in hardware, which has assets and drawbacks. Those drawbacks are significant. Middleboxes specifically produced for ISPs are expensiv both in acquisition and maintainance, also they usually have to be replaced to introduce new features [2]. Also they are difficult to scale with higher or lower demand. All these problems are avoidable through network function virtualization. And the long-term plan is indeed to replace these hardware middleboxes with all-purpose hardware that is cheap and easily replaceable [3]. The networking functions would be implemented in software. 7 of the worlds largest telecoms network operators are in an standards group for virtualization of network functions. So the topic is already being discussed in ISPs [4]

1.2 Goal of the thesis

The goal of this thesis is to test different software Middlebox implementations. We will install different middlebox implementations in our testbed. Then we will test the packet processing capability, try to find bottlenecks for the performance when processing packets. We will evaluate our results. Additionally we want to evaluate if software Middleboxes are competitive with hardware implemented Middleboxes and could replace them in the foreseeable future. ectionOutline

The thesis reads as follows. The second chapter introduces the theoretical concept of NAT and a NAT model which we used in our tests. Also it defines performance testing. Additionally the Data Plane Development Kit is introduced, DPDK. The third chapter informs the reader about the general idea behind our tests. Further it presents the software used for the tests. This includes the software running on the device under test, as well as the software used to run the tests. It explains the methodological approach used in this thesis. Here it explains the setup for the experiment. In chapter 4 are the collected results of the Firewall and NAT tests with a brief analysis of the result. Finally chapter 5 summarizes the outcome and gives possible future works of this thesis.

Chapter 2

Background

This chapter gives a overview over network address translation and the NAT model we will assume in this thesis. Also it will explain our approach to performance testing. Finally the chapter outlines the Data Plane Development Kit, developed by Intel [5].

2.1 NAT

Network address translation NAT was first described 1993 and written into RFC 3022 in 2001. It was proposed as an temporary solution for the shortage of IPv4 addresses. It should slow down the need for IPv4 addresses of private customers and businesses [6]. It does this by working as a connector between 2 different networks with different IPv4 address spaces. Mostly it translates between the address space of the internet and a private network. Since NAT is used so broadly it is one of the most common middleboxes.
NAT in private households is in many instances implemented directly in the router. The home ususally only gets one IPv4 address from its ISP. The router then interconnects the home network to the internet via an ISP. It translates the private IP addresses of the home network to enable them to share the single IPv4 address [6][Page 168]. In corporate networks it basically fulfills the same purpose. The main difference is that the border router manages multiple public IPv4 addresses and manages the correct translation between them and the private IPv4 addresses in the private network. Here we see the simple version with only one public IPv4 address.

A NAT middlebox manages the translation between the different IPv4 address spaces. To achieve this the middlebox has to save a mapping of the private IP addresses to the public ones. In the simplest imaginable case we have as many public IPv4 addresses as we have private ones. In that case the mapping is simply a bijection. When the NAT middlebox receives a packet from a new private IP S in the internal network it maps it

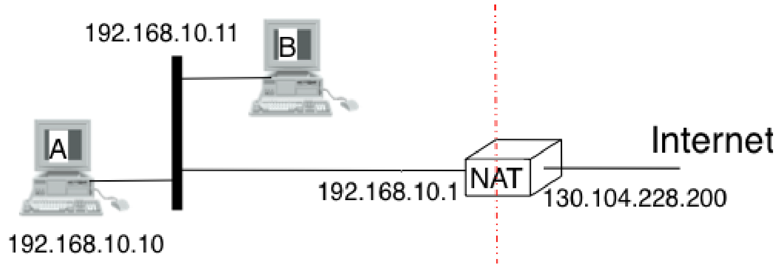

Figure 2.1: A simple NAT with one public IPv4 address [6][Page 168]

to a not used public IP from its address pool. This mapping is saved. To translate the packet the NAT middlebox has to :

1. Replace the original source IP from the packet with the mapped public IP
2. Completely recompute the IP header checksum, as not only the Time To Live header field changes, but also the source IP header field [7][Page 435]
3. Recompute the checksum in the TCP or UDP header if existent. The checksum of these protocols computes the checksum over the whole packet

2.2 NAT model

2.3 Performance testing

2.4 Data Plane Development Kit

Chapter 3

Methodology

3.1 General Idea

3.1.1 Software

3.2 Test Methodology

3.2.1 Experimental Setup

3.2.2 MoonGen Traffic Generator

3.2.3 Open VSwitch

3.2.4 mOS

Chapter 4

Evaluation and Analysis of results

4.1 Firewall tests

4.2 NAT tests

Chapter 5

Conclusion

5.1 Future Works

Bibliography

[1] "Carrier grade network address translation," https://www.a10networks.com/resources/glossary/carrier-grade-network-address-translation, visited: 20.08.2017 13:50.

[2] "Network functions virtualisation," https://portal.etsi.org/nfv/nfv_white_paper.pdf, visited: 20.08.2017 13:40.

[3] M. A. e. a. Joao Martins, "Clickos and the art of network function virtualization," 2014.

[4] "Leading operators create etsi standards group for network functions virtualization," http://www.etsi.org/news-events/news/644-2013-01-isg-nfv-created, visited: 20.08.2017 15:50.

[5] "Dpdk website," http://dpdk.org/, visited: 21.08.2017 15:50.

[6] O. Bonaventure, *Computer Networking: Principles, Protocols, and Practice.* The Saylor Foundation, 2011.

[7] A. S. Tanenbaum, *Computer networks*, 1996, no. 04; TK5105. 5, T35 1996.