Journal of Computer and System Sciences 81 (2015) 981–999

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Improving network intrusion detection system performance through quality of service configuration and parallel technology

Waleed Bul'ajoul [a,*], Anne James [a], Mandeep Pannu [b]

[a] Faculty of Engineering and Computing, Coventry University, Coventry, UK
[b] Department of Computer Science, Kwantlen Polytechnic University, Surrey, British Columbia, Canada

ARTICLE INFO

Article history:
Received 10 March 2014
Received in revised form 12 September 2014
Accepted 22 September 2014
Available online 18 December 2014

Keywords:
Network security
Intrusion detection system
Intrusion protection system
Parallel processing
Switch configuration
Quality of Service

ABSTRACT

This paper outlines an innovative software development that utilises Quality of Service (QoS) and parallel technologies in Cisco Catalyst Switches to increase the analytical performance of a Network Intrusion Detection and Protection System (NIDPS) when deployed in high-speed networks. We have designed a real network to present experiments that use a Snort NIDPS. Our experiments demonstrate the weaknesses of NIDPSs, such as inability to process multiple packets and propensity to drop packets in heavy traffic and high-speed networks without analysing them. We tested Snort's analysis performance, gauging the number of packets sent, analysed, dropped, filtered, injected, and outstanding. We suggest using QoS configuration technologies in a Cisco Catalyst 3560 Series Switch and parallel Snorts to improve NIDPS performance and to reduce the number of dropped packets. Our results show that our novel configuration improves performance.

1. Introduction

In order to provide new developments and highest-quality services, companies implement the latest technologies in their infrastructure. A company's network plays a vital role in its business projects. Keeping the computer network up-to-date with the latest software and security techniques is essential for success and progress. Reliability and safety are the major concerns in enabling a company to achieve success and boost its progress. However, networks can also be considered a major risk in any business project. Security issues have increased as technology has advanced [1]. Fuchsberger [2] reported that, according to a survey conducted by the Federal Bureau of Investigation and Crime Scene of Investigation (FBI/CSI), viruses are behind many attacks on business networks. Moreover, Denial of Service (DoS) attacks and unauthorised user access (which can be initiated from external or internal LAN sources) have also increased dramatically. It is also noticeable that nowadays there are powerful intrusion tools available, allowing hackers to attack networks even if they know little of the software. Attackers can now use several tools simultaneously to achieve an objective. The 9th Annual Worldwide Infrastructure Security Report and ATLAS 2013 data report [3] said the number of Distributed Denial of Service (DDoS) attacks has grown significantly, nearly doubling on a year-to-year basis between 2006 and 2010. The size peak of attacks in 2013 increased by over 200 percent from the previous year, with the largest reported attack at 309 Gbps, and with multiple respondents reporting attacks larger than 100 Gbps, the previous largest reported attack size. Additionally, in

* Corresponding author at: EC building, Coventry University, Priory Street, Coventry CV1 5FB, UK.
E-mail addresses: Bulajouw@coventry.ac.uk (W. Bul'ajoul), a.james@coventry.ac.uk (A. James), mandeep.pannu@kpu.ca (M. Pannu).

http://dx.doi.org/10.1016/j.jcss.2014.12.012
0022-0000/

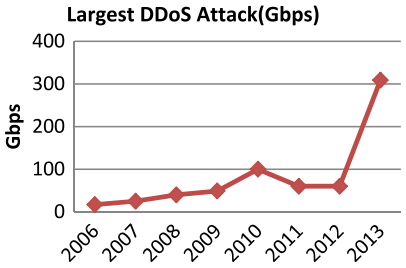

Fig. 1. Largest DDoS attack reported by Arbor networks [2].

2013, ATLAS observed more than 8x the number of attacks over 20 Gbps as compared to 2012 (see Fig. 1). Therefore, security products, such as firewalls, vulnerability assessment tools, antivirus programs, and Network Intrusion Detection and Prevention Systems (NIDPSs), are utilised to reduce the risk of attacks. However, even these measures are not 100 percent effective in protecting networks. One problem is that in heavy traffic, packets can be dropped prior to analysis [4–6]. It is becoming recognised that advantage could be taken of multi-core to overcome the problem of network traffic rate superseding the rate at which NIDPSs can process incoming data [7].

This paper, which builds on our previous work [8], describes research which aims to solve the problem of dropped packets which can be a prevalent issue for NIDPSs used in heavy and high-speed traffic environments. Our research uses Snort IDS (Intrusion Detection System), in Network Intrusion Detection System (NIDS) mode. Snort is currently the most popular NIDPS software. Snort can be installed in any machine and runs on different operating systems such as Windows and Linux. Snort, which was introduced as a lightweight IDS, has developed significantly in the last 10 years. We conducted experiments to test Snort NIDS analysis performance under heavy and high-speed traffic. We also demonstrated that Snort NIDS performance can increase the number of analysed packets and decrease the number of dropped packets using alternative technologies such as a Quality of Service (QoS) configuration and parallel technology.

The remaining part of this paper is organised as follows: Section 2 gives a background about security mechanisms, stages and intrusion detection technologies. Section 3 explains our experimental design and implementation. Section 4 presents the results of the experiments and the evaluation. Then Section 5 gives an overview related work. Finally Section 6 concludes the paper and suggests recommendations and further work.

2. Background

2.1. Security mechanisms and approaches

Security is a major concern in every aspect of our daily life. New methods and equipment are constantly being devised to ensure protection. Computer networks continue to face many threats. We can consider three stages to achieving security in computer system networks: prevention, detection and correction. Prevention stops attacks before they enter system. Detection catches the attacks after they have entered and then Correction rectifies problems, which could be detected attacks or mistakenly prevented non-attacks. Prevention is the ideal solution, as compared to detection and correction, but it is impossible to prevent 100 percent of attacks [9]. Detection techniques provide results that can be used to prevent further attacks and aid correction. Thus the three stages combined offer an effective approach to achieving security. Common security mechanisms are firewalls, antivirus programs and intrusion detection and prevention systems.

2.1.1. Firewall

In order to secure a corporate network or sub-network, network traffic is usually filtered according to criteria such as origin, destination, protocol or service, typically through dedicated routers called firewalls. Firewalls are a common security defence and nowadays are treated as an integral part of every network. A firewall may be software or hardware; its functionality is based on filtering mechanisms specified by a set of rules, known as a policy, which can protect a system from flooding attacks. The fundamental function of a firewall is to sort packets according to allow/deny rules, based on header-filed information. The disadvantage of firewalls is that they cannot fully protect an internal network since they are unable to stop internal attacks. For example, malicious and unwanted web traffic can go through a firewall to strike and damage a protected computer system. A firewall is a set of rules such as to allow or deny protocols, ports or an IP address. Today's Denial of Service (DoS) attacks are too complex for firewalls because they cannot distinguish good traffic from DoS attack traffic [10]. The firewall provides the benefit of added security to strengthen a network when used in conjunction with an IDS.

2.1.2. Antivirus programs

Computer viruses are programs which cause computer failure and damage computer data. Especially in a network environment, a computer virus poses an immeasurable threat and can be very destructive. Antivirus programs are software that can be installed onto a computer in order to detect, prevent and make decisions regarding whether to quarantine or