L-004

High-Performance Distributed NIDS Cluster Based on Hybrid Detection Platform

Zhenguo Hu† Hirokazu Hasegawa† Yukiko Yamaguchi† Hajime Shimada†

1. Introduction

Nowadays, high throughput network traffic is gradually becoming commonplace. For this reason, the demand for a high-speed Network Intrusion Detection System (NIDS) is increasing and some of them works as Intrusion Prevention System (IPS). How to protect the network security and detect malicious or suspicious traffic attacks on network users has become the common goal of researchers on the whole world. NIDS is an efficient security technology, which can be used for the security detection of malicious or suspicious traffic in the network, and can also for the security protection of the host. Currently NIDS is widely used at border of the Internet and Intranet. It can be used not only to detect external attacks from the Internet, but also to help detect threats directly from the Intranet. By comparing different traffic characteristics in the system, it can screen out intrusion methods, and take corresponding security protection measures. Traditional NIDS distinguishes the malicious or suspicious packets among the received network packets based on predefined rules that define the communication pattern of the malicious packets [1]. It has good detection performance and low cost in less than 10Gbps network environment. For example, the IDS/IPS appliance that have 2-3Gbps IPS throughput even in hundreds of JPY cost. It is usually used in the Internet environment.

Compared with the traditional NIDS which focuses on the Internet, Intranet traffic inspection NIDS becomes more important in order to tolerate Advanced Persistent Threat (APT). APT usually occurs in the Intranet environment and will continue to threaten the internal network security of enterprises. Since the attack occurs from the inside, it will not only cause greater property losses to the enterprise, but also be more difficult to detect and defend. There are also some researches which are used for Intranet inspection for APT. For instance, Hasegawa et al. has proposed itinerancy inspection of Intranet considering seriousness of inspection [2]. However, with the rapid development of intra network bandwidth, internal inspection gives ten times larger traffic to NIDS, the traditional NIDS has been unable to deal with such a large amount of traffic in terms of hardware, software and architecture under a lower commercial cost. It will suffer from serious packet loss, resulting in a large number of wrong reports.

In order to deal with tens of Gbps network traffic in a cost-effective method, researchers have made a lot of attempts, but there are still a lot of limitations. The first challenge is how to collect data packets in such a huge throughput with a lower cost approach. When each packet arrives at NIC, it will produce a DMA interrupt, and the packet will go through two memory copies from NIC to kernel space, in that case it will cause performance degradation. Next challenge is the process of feature matching which is the most time-consuming process, it will mostly decrease the inspection speed. In order to realize the detection of large-scale traffic, high throughput NIDS is already used in enterprise usage, it is usually configured with a single computing platform which must use powerful computing chips. This kind of NIDS will put a lot of pressure on the detection platform and greatly increase the economic cost. In that case, cost-effective NIDS is required to achieve internal inspection even in small to medium size organization.

In this paper, we try to design a cost-effective high-performance distributed cluster based on hybrid detection platform. A high-speed network distribution switch will distribute the different traffic to the hybrid IDS cluster, and the cluster will do the deep inspection for the packet in order to prevent the network malicious attack from causing damage to the Intranet environment.

2. Proposed Method

This system is designed to improve the performance of NIDS with a cost-effective way under high-speed network environment, it is divided into two different parts: high-speed network distribution switch and hybrid IDS cluster. The system architecture is shown in Figure. 1. The traffic firstly pass through the network distribution switch, in this process it will also do some light traffic inspection simultaneously. Then the traffic will be mirrored to the hybrid IDS cluster according to different traffic size for further detection. The large traffic and medium traffic will be processed by FPGA and GPU. The CPU will also process some small network traffic to save the resource.

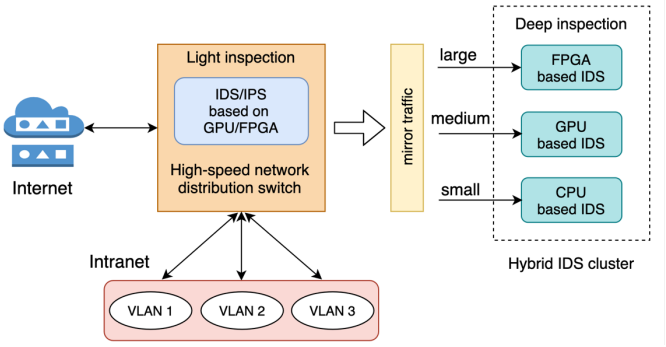

Figure 1. System Architecture

2.1 High-speed Network Distribution Switch

In the high-speed network distribution switch, the traffic from the network will firstly be processed by a GPU based IDS to achieve light inspection, then according to the different packet or session size, it will be mirrored and distributed to the hybrid IDS cluster.

† Nagoya University

To achieve this goal, on the one hand, it is necessary to use GPU to achieve rapid detection of large-scale traffic. Since the network distribution switch is the main entrance of the traffic, compared with the accuracy of detection, speed and real-time are the main goals of this IDS. One of the most effective way to strengthen the speed and real time is to employ GPU to accelerate the signature-based IDS. In the signature-based IDS, the most time-consuming process is pattern matching, it will take up a lot of computing resources. As a general graphics processing device, GPU has powerful parallel computing ability and great advantages in performing the similar tasks. It is useful to help to accelerate the pattern matching process, the entire task will be divided into different small tasks to run on different GPU cores.

On the other hand, after checking the network traffic, it is also important to forward the traffic to the IDS cluster in order to do the deep inspection. DPDK is a great method to decrease the forwarding time. Unlike the data forwarding in Linux system, DPDK focuses on high-performance traffic packet processing in network applications. By combining the DPDK with Network OS, during the process of data transferring, the kernel can be bypassed to accelerate the transferring speed.

In order to reduce the difficulty of designing the whole system development, we plan to firstly verify the feasibility of the system based on the software platform, and then gradually migrate to the hardware platform to achieve efficient detection of the suspicious network traffic. We will employ SmartNIC, GPU and x86 based system to complete the high-speed network traffic distributing and mirroring. After verifying the system can work well, the FPGA chip is used to achieve a hardware based high-performance network traffic distribution switch. We plan to design and use a hardware which includes a core FPGA high-performance chip, QSFP transceiver and the ARM coprocessor. FPGA chip is used to complete light inspection and traffic distributing and switching, QSFP transceiver is used to transfer the network traffic to the IDS cluster, and the ARM coprocessor is employed to achieve DPDK protocol with FPGA chip.

2.2 Hybrid IDS Cluster

After sending the network traffic to the IDS cluster, in order to take advantage of different processing units and greatly cut down the commercial cost, a hybrid IDS acceleration platform is built to further detect traffic packet. This platform consists of three different acceleration detection methods, FPGA, GPU and CPU. Three different kinds of NIDS will be formed into a heterogeneous IDS cluster, through load balancing the network traffic will be distributed to different NIDS, using their different characteristics to achieve the packet deep inspection. An important reason for using this platform is to fully balance power consumption, performance and cost, in that case it will optimize the energy consumption and performance balance by using the different characteristics of each acceleration platform in a cost-effective method. We hope that the whole system can be implemented in a highly integrated approach.

FPGA has the characteristics of low power consumption and strong performance, it has the most excellent energy efficiency ratio. By programming the internal circuit of FPGA chip, compared with software platform, the corresponding algorithm can be implemented with hardware circuit which greatly speed up the computing process of traffic inspection. For the signature matching process, we plan to use this acceleration NIDS to achieve deep inspection. The decoding of network traffic and pattern matching will be implemented on the hardware circuit of FPGA chip.

For the medium network traffic, we plan to use GPU acceleration platform. GPU has the advantages of powerful parallel computing ability and large capacity cache, which is very suitable for accelerating neural network computing. Therefore, in the GPU based NIDS, we plan to adapt machine learning to detect the suspicious traffic. At the same time, we will employ deep model compression technology such as pruning and quantization to accelerate the inference speed. By quantizing the deep learning networks, it can increase throughput, reduce resource utilization, and deploy larger networks onto smaller target boards to decrease the inference time.

As a general processor, CPU is not as powerful as FPGA and GPU, but its low power consumption and high flexibility are still suitable for small-scale network traffic detection. We plan to use a general CPU to achieve the maximum network traffic detection with lower power consumption and device cost.

3. Conclusion

In this paper, we plan to design a high-performance distributed NIDS cluster which is based on a hybrid acceleration platform in a cost-effective approach, the traffic from both the Internet and Intranet are firstly handled by light IDS to achieve the rapid detection speed. If the network bandwidth exceeds the processing capacity of light IDS, the traffic will be transmitted to the hybrid IDS cluster through the high-speed network distribution switch to complete deep packet detection. The whole system is expected to achieve the detection speed in tens Gbps to 100Gbps, we hope that through this system gives cost-effective network protection with small to medium size organization.

Reference

[1]J. Kim, J. Park, “FPGA-based network intrusion detection for IEC 61850-based industrial network”, ICT Express,Vol.4, Issue 1 (2018).

[2]H. Hasegawa, et al. “An Incident Response Support System Based on Seriousness of Infection”, ICOIN2016, pp. 69-74 (2016).