Chapter 14
A Fireworks-Based Approach for Efficient Packet Filtering in Firewall

Sreelaja N. K.
PSG College of Technology, India

ABSTRACT

Information protection in computers is gaining a lot of importance in real world applications. To secure the private networks of businesses and institutions, a firewall is installed in a specially designated computer separate from the rest of the network so that no incoming packet can directly get into the private network. The system monitors and blocks the requests from illegal networks. The existing methods of packet filtering algorithms suffer from drawbacks in terms of search space and storage. To overcome the drawbacks, a Fireworks-based approach of packet filtering is proposed in this chapter. Termed Fireworks-based Packet Filtering (FWPF) algorithm, the sparks generated by the fireworks makes a decision about the rule position in the firewall ruleset matching with the incoming packet. The advantage of FWPF is that it reduces the search space when compared to the existing packet filtering algorithms.

INTRODUCTION

In real world applications, information protection in computers is gaining a lot of importance. Logical security system such as firewall is made use of in such systems. To secure the private networks of businesses and institutions, firewalls are the crucial elements. A firewall is a set of related programs located at a gateway server that protects the resources of a private network from the users of the external network. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming packet can directly get into the private network. The firewall monitors and blocks the requests from illegal networks (Sreelaja & Vijayalakshmi Pai, 2010).

Packet filtering performance of basic firewalls largely affects the throughput of a network protected by the firewall. Packet filtering (Eyadat, 2008) refers to accept or block incoming packets based on the filtering rules defined in the ruleset. A filtering rule is a multidimensional structure where each dimension

DOI: 10.4018/978-1-7998-1659-1.ch014

is a set of network fields and an action field. The network field denotes source IP address, destination IP address, source port and destination port. The action field for each rule is accept or drop based on which the incoming packets are filtered. An accept action allows the packet access into the protected domain. A drop action causes a packet, in violation of the security policy, to be rejected. The filtering rules in the ruleset can be any or all of the combination of source IP address, destination IP address, source port and destination port. A filtering rule is said to be matching filter for an incoming packet if all the fields in the filtering rule matches with the corresponding fields of the incoming packet header.

In this chapter, a Fireworks based approach for filtering the incoming packets in a network based on the filtering rules in a rule set is proposed. Termed Fireworks based Packet Filtering (FWPF) algorithm, a firework is exploded at a point in the ruleset and the sparks generated by the fireworks fall at several positions on the filtering rules in the firewall ruleset. The sparks are traversed to make a decision about the rule position in the ruleset matching with the incoming packet. This approach provides an optimized search technique to find the positions of the filtering rules in the ruleset matching with the incoming packet. The advantage of FWPF algorithm is that the incoming packets are filtered strictly according to the filtering rules in the ruleset. It is shown that FWPF algorithm scales well in terms of number of searches when compared to sequential search even for a very few number of rules in the ruleset. Also, it is shown that the drawbacks in other existing packet filtering methods are overcome by FWPF algorithm.

RELATED WORK

Mohammad M. Masud, Umniya Mustafa, Zouheir Trabelsi. (2014) have proposed a data driven packet filtering approach. According to this approach, each rule in the rule set is considered a class. The training dataset contains a packet header info and the corresponding class label. Then the classifier is used to classify new incoming packets. The predicted class is checked against the packet to see if this packet really matches the predicted rule. If yes, the corresponding action of the rule is taken. Otherwise, the traditional way of matching rules is followed. The advantage of this data mining firewall is that it offers a much faster rule matching. It is proved that the classifier can achieve very high accuracy of 98% or more, thereby making firewall six times or more faster in making filtering decision.

Trabelsi, Zhang, & Zeidan, (2012, October) have proposed a Packet Filtering Optimization Using Statistical Traffic Awareness Test to improve firewall packet filtering time through optimizing the order of security policy filtering rules and rule-fields (Trabelsi, Zhang, & Zeidan, 2012). The proposed mechanism is based on reordering rules and rule-fields according to packet matching and non-matching histograms, respectively. The current and previous traffic windows statistics are used to check the system stability using Chi-Square Test. If the system stability test indicates that the firewall is stable the same current rule and/or rule-fields orders are used for filtering the next traffic window. Otherwise, an update of the rule and/or rule-fields order structures is required for filtering the next traffic window. However, there is an error precision rate according to this method and 100% classification accuracy is not possible.

Hazem Hamed, Adel El-Atawy, Ehab Al-Shaer (2006) have proposed an Adaptive Statistical Optimization Techniques for Firewall Packet Filtering that introduce a minimal overhead on the firewall processing to allow rejecting the maximum number of the packets as early as possible, thereby reducing the matching time significantly. According to this approach, the space complexity is bounded by O (n), and computational complexity is O (n log n).