Research on a Supervision System for Stateful Firewall Security Configuration based on Markov Chain

Cao Bo, Meng Haohua, Yang Shan, Gao Fei

(Information & Communication Branch of Hubei EPC, Wuhan, China)

Keywords: Markov Chain; queuing theory; firewall rules; access control

Abstract: This article takes security configuration supervision of firewall as the research object, and proposes a supervision scheme of stateful firewall security configuration based on Markov Chain. As stateful firewall is a new type, traditional security configuration algorithm do not apply to its rule set comparison. The stateful firewall based on Markov Chain transforms the rule set into equivalent stateful firewall decision diagrams, and is applied to the stateful firewall rule set comparison. Both theoretical analysis and simulation results have shown that this method can effectively detect all the exception rules between the rule sets.

Introduction

Firewall has a great application value in network security. Therefore, its security configuration has been one of the most basic requirements to perform access control. According to the rule set of access control, security configuration can be divided into security policy configuration and security management configuration[1]. Security policy configuration of firewall rule set is particular important in terms of the following two aspects. How to undertake a safe configuration of firewall rule set has become an urgent practical problem to be solved[2] [3][4]. This article will use stateful firewall to handle it.

Stateful firewall is developed on the basis of that of packet filtering and of application proxy. Liu et al.[5][6] put forward a method of Firewall Decision Tree (FDT in abbreviation) on the basis of FDD. According to Qin et al. [7], there is less research on comparison between firewall rule sets, who put forwards a method of Stateful Firewall Decision Diagram (SFDD in abbreviation) in order to solve the comparison problem. The idea running through this article to solve this problem is as follows: Take use of stateful firewall to give a formal description of the rule sets with the help of Markov Chain. Achieve effective detection of the rule sets of stateful firewall. Meanwhile, improve detection efficiency of safety configuration of firewall rule sets.

Security Configuration Scheme of Stateful Firewall based on Markov Chain

The construction is carried out in follow steps in total:

Step 1. Construction of equivalent decision path f of the stateful firewall.

The rule set of the stateful firewall is assumed to be $\langle r_1, r_2, \mathbf{L}, r_n \rangle$. The firewall undergoes the transition of equivalent decision path from the first rule in the rule set, adding $r_2, \mathbf{L}, r_n$

into f successively. Finally obtained is the equivalent decision path f of the rule set of sta teful firewall.

Step 2. Construction of equivalent decision path *f'* of data packets.

When a data packet arrives in the stateful firewall, a state is generated with the rule set as: $r_k[F_1] \wedge r_k[F_2] \wedge \mathbf{L} \wedge r_k[F_n] \rightarrow action$. The firewall undergoes the transition of equivalent decision path from the first rule in the rule set, adding $r_2, \mathbf{L}, r_n$ into f successively. Finally obtained is the equivalent decision path f of the rule set of the stateful firewall

Step 3. Comparative operation and detection for anomalies of equivalent decision path f of the stateful firewall and of equivalent decision path *f'* of data packets.

This step judges whether there is an anomaly with the rule in the rule set of the此stateful firewall through a comparison between the leaf nodes of equivalent decision path f of the stateful firewall and those of equivalent decision path f of data packets. $C_r^i (1 \le r \le m,\ 1 \le i \le n)$ is used to denote the value of the leaf node on the equivalent decision path, wherein m denotes the number of the leaf nodes on the equivalent decision path and n the number of the rules in the rule set of the firewall.

To judge whether there is abnormality with the rule is to calculate the value of the leaf node C_r^i both on the equivalent decision path f of the stateful firewall and on the equivalent decision path of data packets. If the calculation result is: (1)$\exists r,\ r'$, and makes $C_r^i = C_{r'}^i$, then it can be determined that the filtering rules of r and *r'* are consistent and that there is no rule abnormality in the stateful firewall, which means that the detected data packet is to be released; (2)$\exists r,\ r'$, and makes $C_r^i \neq C_{r'}^i$, then it can be determined that there is inconsistence between rules r and *r'* and that there is rule abnormality in the stateful firewall, which means that the detected data packet is to be blocked.

Step 4. Detection and correction for logic and operation anomalies of equivalent decision path f of the stateful firewall and of equivalent decision path *f'* of data packets.

This step can correct rule anomalies in the rule set through logic and operation of equivalent decision path f of the stateful firewall and of equivalent decision path *f'* of data packets. Here $f \wedge f' \Leftrightarrow \sum_{i=1}^{n} \left(C_r^i \wedge C_{r'}^i \right)$ is used to denote logic and operation between both rules and values of leaf nodes on the equivalent decision path.

To judge whether there is detection and correction of rule anomalies of the stateful firewall is by the calculation of the value of the leaf node C_r^i on the equivalent decision path f of the stateful firewall and of equivalent decision path *f'* of data packets. If the calculation result is: (1)$C_r^i = C_{r'}^i$ or $C_r^i \wedge C_{r'}^i = 1$, then it can be determined that the filtering rules of r and *r'* are consistent and that there is no rule abnormality in the stateful firewall, which means that the detected data packet is to be

released; (2) $C_r^i \neq C_{r'}^i$ or $C_r^i \wedge C_{r'}^i = 0$, then it can be determined that there is inconsistence between rules *r* and *r'* and that there is rule abnormality in the stateful firewall, which means that the detected data packet is to be blocked. At this point, it is necessary to do rule correction, which method is changing the value of the nodes of C_r^i and $C_{r'}^i$ from 1 to 0. This way enables crossing or overlapping rules to have the same filtering field, thus eliminating abnormal rules.

A Supervision Instance of Stateful Firewall Security Configuration

Experiment configuration

The security of the firewall should meet the following conditions: (1) preventing access of data packets from any malicious domain in external network; (2) enabling mail severs with network address such as 192.1.2.3 to receive emails; and (3) authorizing mutual communication between local and remote hosts only initiated by the local hosts.

Detailed experiment configuration is shown in figure 1. The stateful firewall is installed in the gateway router, which has two ports numbered 0 and 1 for external and internal network respectively.

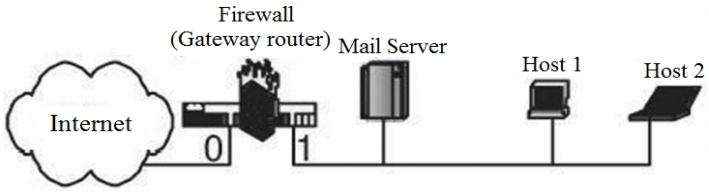

Fig.1 Comparison Instance of Stateful Firewall Rule Set [7]

Actual system performance

According to the study of Chen et al. [8], the number of firewall rules in actual use is up to 3000. Therefore, it is set as 3000 in the initial configuration in this article to meet the requirement of practical use. In addition, during the experiment, the stateful firewall is generated randomly according to characteristics of classification of data packets announced by Launay [9]. The fields of the packets arriving in the firewall include: interface (I), source network address (D), destination network address (D), ID number (N) and protocol type (P). The actual system performance is illustrated in figure 7 below.

After running the client port, the system shows daily check as shown in figure 2. A click on Immediate Check can run a comprehensive examination of the system.

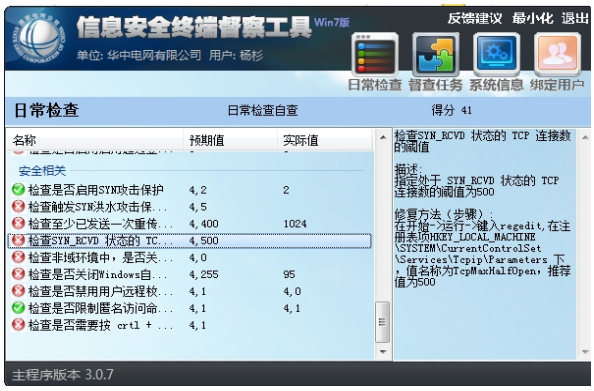

Fig.2. Daily Check Items of Stateful Firewall

In terms of the check information items, a click on the check item can display its description and repair method in the right window as shown in figure 3.

Disable **Guest** Account

Description:
Check if guest account is disabled

Repair method (steps):
Go to Control Panel→ Administrative Tools→ Computer Management→ System Tools→ Local Users and Groups→ Guest Account→ Properties→ Set Disabled

Fig. 3. Description and Repair Method of Check Item of Stateful Firewall

For an already done task, if it was performed before, its specific check details can be reviewed with a click on it, as show in figure 4.

Fig.4. Specific Supervision of Stateful Firewall

Conclusions

This article has proposed a security configuration algorithm of stateful firewall based on Markov Chain and put it into the comparison between rule sets of the stateful firewall. Both theoretical and experimental results have shown this algorithm can detect anomalous rules in the rule set of the stateful firewall and display the detection result in a dynamic and time saving way. It can be certain that research on security configuration of stateful firewall will develop more specifically with the development of network. The next direction will be the optimization of rule sets of multiple stateful firewalls and the method for comparing them.

Acknowledgment

This article is supported by Natural Science Foundation of Shandong Province (No.ZR2014FL012) and Open Fund of Shandong Key Laboratory of Intelligent Computing Technology of Network Environment.

References

[1]Fei Tang. Method of Firewall Configuration Checking based on Regular Expression [J]. Railway Computer Application, 2015, 24(2): 22-27.

[2]Angang Tang, Yongbo Chen, Donghong Ji. A Distributed Firewall Rules Validity Detection Algorithm [J]. Microelectronics & Computer, 2015, 32(2): 5-9.

[3] Lin Li, Xianliang Lu, Zeping Li. A Rule Sets Comparing Algorithm for Diverse Firewall Design [J].Journal of Sichuan University (Engineering Science Edition), 2009, 41(5): 111-113.

[4] Liu A X, Gouda M G. Diverse firewall design[J]. IEEE Transactions on Parallel and Distributed Systems, 2008, 19(9): 1237-1251.

[5] Liu A X, Gouda M G. Complete redundancy removal for packet classifiers in TCAMs [J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(4): 424-437.

[6] Liu A X. Firewall policy change-impact analysis [J]. ACM Transactions on Internet Technology, 2012(3): 2122-2128.

[7] Zheng Qin, Yijun Li, Lu Ou, Alex X. Liu. A New Approach To Compare Firewall Rule Set based on SFDD [J]. Journal Hunan University (Science Edition), 2014, 41(10): 103-107.

[8] Chen F, Liu AX, Hwang J, et al. First Step Towards Automatic Correction of Firewall Policy Faults [J]. ACM Transactions on Autonomous and Adaptive Systems, 2012, 7(2): 1-24.

[9] Launay A. High level firewall language [EB/OL]//[2012-10-28] http://www.hlfl.org.