Audit and Processing of Anormaly Firewall Rules

Bo Cao
Information communication company
State Grid Hubei Electric Power Company
Yichang, China
E-mail: ycgaofei@163.com
Corresponding Author

Zheng Yu
Information communication company
State Grid Hubei Electric Power Company
Yichang, China
E-mail:ycyuzheng@163.com

Fei Gao
Information communication company
State Grid Hubei Electric Power Company
Yichang, China
E-mail: yccaobo@163.com

Abstract—1. Objectiv： Firewall rules configuration has been the focus of network security research and this paper studies and improves the firewall rule audit method to improve the matching efficiency of firewall rules. 2. Method: This paper makes a detailed study of the relationship between firewall rules, and explain them by the concept of the collection, then summarizes anormaly conflicts, then the rule of the firewall is optimized by using statistical algorithm. 3. Results: This paper designs the hierarchical audit structure, simplifies the audit work, and applies the policy tree algorithm to audit the rule set of the firewall. At last, the model of the different anomaly is given. 4. Conclusion: The 7 anormalies in the experimental rule set are all discoveried, and the average matching times is reduced from 4.624 to 3.544.

Keywords- Firewall; rule set; anormaly; audit; policy tree

I. INTRODUCTION

As the only entrance between intranet and extranet, the firewall has protected the internal network from outside invasion, and its performance have a significant impact on the effective data transmission network. How to prevent the firewall becomes the bottleneck of the network communication is always the focus in the field of network security, the problem mainly focus on the confliction between firewall rules, that is, the problem of rules anormalies. Whether the firewall configuration rule is reasonable or not is directly related to the security of the firewall, and the security of the whole network. Firewall policy audit can find the problem of the configuration, and improve the protection performance of the firewall. The rule configuration of the firewall should satisfy 3 conditions: consistency, integrality and tightness, In this paper, the firewall decision diagram is adopted to represent the initial configuration of the firewall, and the optimization is ensured, and the three conditions of the firewall rule configuration are ensured[1].

II. FIREWALL CONFIGURATION RULE STRUCTURE AND RELATIONSHIP

Rules are the basic elements of the firewall security policy, and usually the firewall policy is composed of dozens to thousands of rules. In order to analyze the security policies of the firewall, and audit the firewall configuration policy, it is needed to define the relationship between the rules.

A. Structure of firewall rules

The firewall strategy is a list of orderly linked lists of filter rules. Each filtering rule contains several network domains, which usually consist of six domains: protoco1, source IP address, source port, destination IP address, destination port, action[2], which is shown in Table Ⅰ:

TABLE I. FIREWALL RULES STRUCTURE

Firewall rules structure	Field name	Value
1	Index	i=1,2,3…n
2	Protocol	TCP、UDP
3	Source Address	0.0.0.0~255.255.255.255
4	Source port	0.0.0.0~65535
5	Destination address	0.0.0.0~255.255.255.255
6	Destination port	0.0.0.0~65535
7	Action	Accept, Deny

Index describes the location of the rule in the rule concentration; Protocol defines transport layer protocols; The source address and destination address denote the sender IP address and the IP address respectively, and the source address can be both a host address (e.g. 135.12.44.254) and a address range (135.24.44.*); Similar to IP address, the source and destination ports can either be a specific port number or any port. Action is similar to Boolean accept or deny. When the action executes accept, the firewall releases packets, on the contrary, the firewall refused the packet passed.

B. *Relationship between firewall rules*

The firewall performs a matching detection for the received packets by above rules, and the data that each rule matches can be regarded as a collection, so the relationship among the rules can be transformed into the relationship between the sets. According to the concept of collective, the relationship between any two non empty sets can be divided into inclusion, inclusion, separation, equality and intersection[3,4].

Assuming Sxis a set that the rule Rx matched, and BeforeSx is a set that any rule before Rx, then

In_Sx= Sx ∩ BeforeSx，

Com_BeforeSx= BeforeSx - In_Sx,

Com_Sx=Sx- In_Sx

In the above formula In_Sx is the intersection of Sx and BeforeSx, Com_Sx is the complement of Sx to In_Sx, Com_BeforeSx, Com_Sx is the Complement of BeforeSx to In_Sx.Then these five relationship can be expressed as the following:

Contain ： In_Sr≠0 and Com_BeforeSr=0 and Com_ Sr≠0.

Included：In_Sr≠0 and Com_BeforeSr≠0 and Com_ Sr=0.

Separate：In_Sr=0.

Intersect：In_Sr≠0 and Com_BeforeSr≠0 and Com_ Sr≠0.

Equal：Sr = BeforeSr.

III. ANORMALY RULES ANALYSIS

Essentially, anormaly rules is vague classification problem, usually due to the rules of the field between two or more overlapping result, and that causes firewall security vulnerabilities [5]. The validity of a rule in the rule collection can not ensure the overall effectiveness of the rule set, which is the network management most concerned. Next, this paper summarizes some of the common anormalies at regular kind by analyzing the relationship between the two rules.

A. *Shield anormaly*

In the Firewall Policy table, if rule s prior to rule *r*, and the packet that be matched by both *r* and *s* ,then rule *r* is shield by rule *s*, and the rule *r* that be masked is equivalent to a failure rule[6,7].

B. *Intersection anormaly*

If the action domains each belong to rule r and rule s are different, and there exists the intersection between *r* and *s*, then the two rule is intersected. At the same time, if *r.action ≠s.action* is established, then the rule *r* and *s* are intersection anormaly.

C. *Redundancy anormaly*

If the rule r and rule s match the same data packets, and execute the same action, the rule r is redundant. In this case, the lack of rule r has no effect on the security policy, but the reservation of r can cause the rule redundancy.

These three anomalies usually appear more frequently, and it is possible to appear when each rule is independently configured, so it is the focus of the audit process.

IV. FIREWALL POLICY AUDIT SYSTEM DESIGN

A. *Audit scheme which based on policy tree*

Policy tree is also called judging tree, it is a kind of graphics tool that describes processing, it is suitable for describing problem which has multiple judgments, and each decision is related to several conditions. Policy tree is a tree structure, similar to the flow chart. Each tree node represents a decision of one attribute in the process, each branch represents an output of a decision result, each leaf node represents the final class distribution, and decision process is started by the root node[8].

In order to simplify the algorithm, only the 5 domains of the rules are considered in the rule collision detection: src_ip, dest_ip, src_port, dest_port and protocol[9]. The src_port and dest_port may range from 0~65535, while the actual application typically takes only a limited range. Suppose the existing firewall policy configuration is composed of n rules, denoted as r1,r2…rn,and each rule's filtering domain <protocol，src_ip，src_port，dest_ip，dest_port>denoted as F, F2…Fm.

Take rule ri and rj as an example: Step1:Compareing the protocol domain F1 each belong to ri and rj.that step is represented by the root node in the policy tree and the 4 decision output of the root node is as follows:

1) $r_i[F_1]$ *is a proper subset of* $r_j[F_1]$*;*
2) $r_i[F_1]$ *is a superset of* $r_j[F_1]$*;*
3) $r_i[F_1]$ *is a sameset of* $r_j[F_1]$*;*
4) $r_i[F_1]$ *is not related to* $r_j[F_1]$*;*

Step2: Comparing ri [F2] and rj.[F2] in branch 1,2,3, And according to the different results of the comparison , algorithm repeat above steps to create new branches, until the final comparison results are generated[7,10]. There is no intersection between 4 branches, so the two rule protocol domains are not relevant, and the two rules is no conflict, the comparison ends. As it is shown in Fig.1:

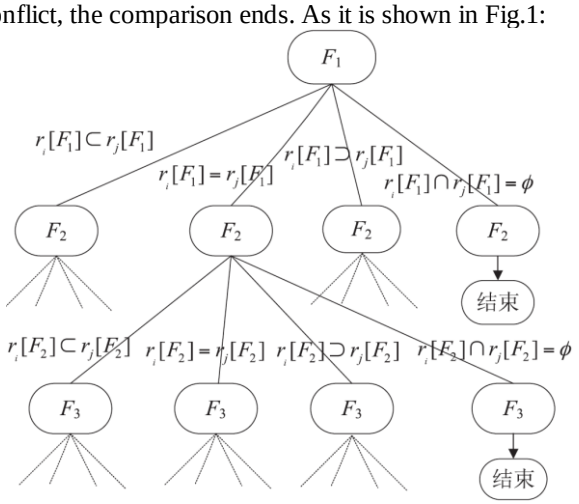

Figure 1. Algorithm structure of anomaly detection for policy tree

According to the Fig .1,the algorithm inspects rules by sequence of protocol domain-source lP address-source port-destination IP address-destination port-action area whether there are intersection parts on the path of the policy tree. If there are intersection in the policy tree path, there may be anormaly, and the type of anormaly can be judged according to the preceding anormaly definition.

B. *Improved policy tree audit algorithm*

In the traditional policy tree, a large number of branches and judgment logic are appeared in the process, and the efficiency of the audit is slow down. This paper improves the audit scheme of the policy tree, and effectively improves the matching speed of the firewall rule set.

In the process of the actual operation of the firewall, single configuration rules do not vary greatly, the configuration parameters often in the same limited range[11]. and redundant anormaly rule is often a minority in rule set, so it is very inefficient to detect each rule for anormalies. By using the filtering mechanism of the firewall itself, establish a policy tree that contains the standard configuration range of all the rules, then compare each configuration rule of the firewall with the policy tree, and classify the rules according to the results. In this process, a single rule's anormalies can be found. After the classification, the conflict detection will be executed and the audit efficiency is greatly improved[12].

Similar to the traditional policy tree, the new algorithm still chooses src_ip/dest_ip, src_port/dest_port and protocol as filtration options. This paper selects the protocol domain, src_ip and dest_port as an example to expounds the improved algorithm flow.

Suppose the rules which will be Audited are r1,r2…rn, then the improved audit scheme is as follows. Firstly, a rule ri is contrasted with a standard policy tree to determine its class. The main types include user management, communication, access control, object group, and pre classification. The process is as follows.

1) protocol comparison

Because the same branching processes contain rules with the same protocol domain, and in order to reduce the number of comparisons of the unrelated rules, so it should be the first that rule's protocol domain to be judged. After this step, the algorithm continues down the policy tree.

2) Comparison of the source IP

The comparison of the r_i's source IP and Src IP node of standard policy tree can find the matching range. Then if the source IP range of configurations exists risk and other issues, it will list the results that are the risks of the policy which may have caused, and go ahead, and the algorithm then proceed down[13,14].

3) Comparison of the destination port

Because the value of the destination port field is limited, in the comparison process of Rule port and the standard policy tree use destination port classifying rules again to reduce the number of follow-up traversal, and further reduce the time complexity of the algorithm. Comparing the r_i's source port with the each node of the standard policy tree to find the node corresponding to the range r_i belongs. It will list the results of the risks which are the matched risk nodes which may have caused.

4) r_i is summarized into the corresponding categories

After the comparison of the rules, the rules are already listed in each category, and then the rules of the same category are to be carryed out conflict redundancy detection by policy tree audit program. Finally, the final audit report is provided with the results of the above steps and the redundancy detection of the conflict.

The improved audit algorithm uses the classification method, so that the comparison of the rules is limited to a certain kind of category, which reduces comparison times and greatly improve the efficiency of the comparison operation[15,16,17]. On the other hand, the problems existing in the single rule can be discovered though the process of pre classification, and the algorithm also set up the audit operation for a single rule.

C. *System design*

This system demonstrate the network topology structure by network topology discovery technology, the user can choose the configuration file that needs to load, after the analysis, system create audit tasks and start audit module. The user selects the rule that needs to audit in the audit policy database, and then adds it to an audit rule group. System parses the rules one by one, and the audit results are written back to the database storage. Finally, it will be demonstrated as a report in the foreground interface.

The structure of this system is divided into three layers, that is, the data collection layer, the analysis processing layer and the management display layer. As it is shown in Fig.2:

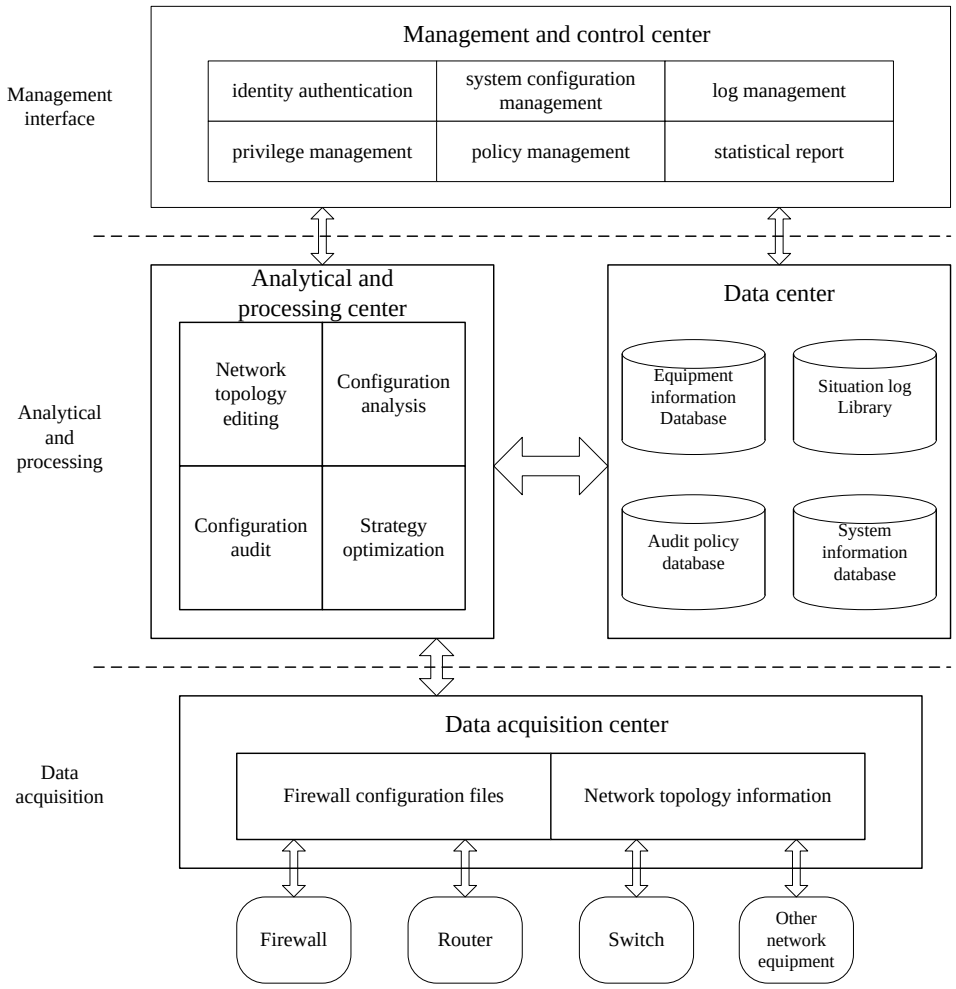

Figure 2. structure of firewall audit system

The following figure is the system control interface:

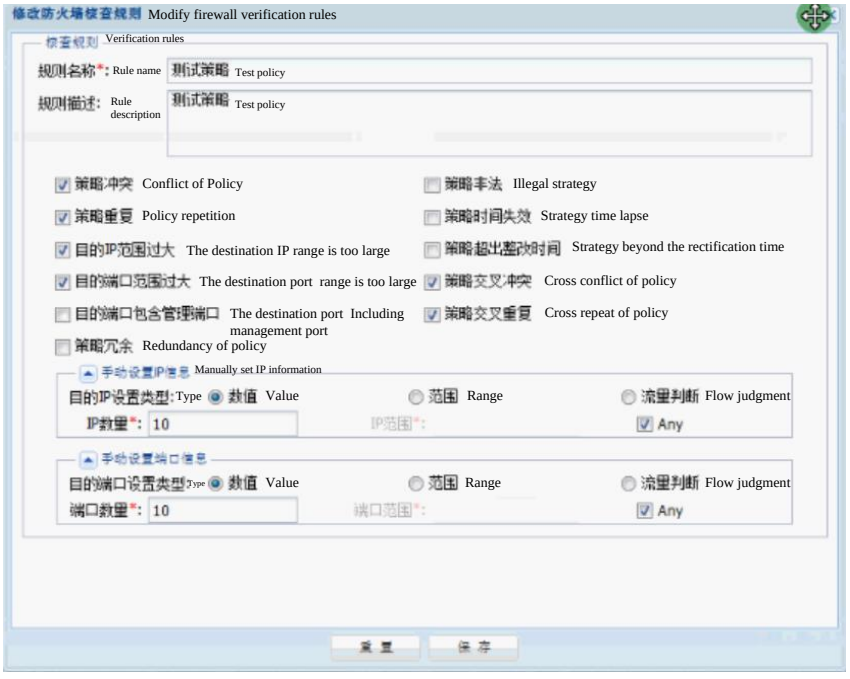

Figure 3. Firewall audit system control interface

V. SIMULATION EXPERIMENTS AND ANALYSIS

This paper selects the test rule set which covering the all types of conflict, and in order to resemble the actual network conditions, a large number of data packets are matched to several rules. Take the TCP table as an example, the initial rules set is shown in Table 2:

TABLE II. INITIAL RULES SET

Order	S_ip	S-port	D_ip	D_port	Action	Time
1	152.7.57.0-152.7.57.255	120-655	187.187.0.48	0-680	Deny	5
2	152.7.57.135-152.7.57.135	150-450	187.187.0.34-187.187.0.34	220-800	Accept	1
3	152.7.57.136	30-90	187.187.0.35	220-800	Deny	4
4	152.7.57.0-152.7.57.255	40-360	187.187.0.0-187.187.0.255	50-300	Deny	9
5	152.57.186.0-152.57.186.255	40-60	121.128.0.0-121.128.255.255	60-560	Accept	12
6	206.220.0.48-206.220.255.255	0-220	121.187.0.45-121.187.0.255	20-80	Accept	3
7	187.187.0.44-187.187.255.255	680-1280	121.10.7.0 -121.10.7.255	12-56	Accept	9
8	187.187.0.48-187.187.0.54	680-1280	121.10.7.58-121.12.7.60	220-800	Deny	5
9	187.187.0.48	100-700	121.10.7.58-121.12.7.60	22-400	Deny	4
10	187.187.0.48-187.187.0.50	200-500	121.10.7.59-121.12.7.66	40 -550	Accept	6
11	46.152.93.0-46.152.93.255	100-655	121.187.57.0-121.187.57.255	24-120	Accept	8
12	187.187.0.100-187.187.0.120	100-405	121.10.7.0-121.12.7.255	15-500	Deny	6
13	187.187.0.112-187.187.0.113	100-200	121.10.7.58-121.12.7.60	90-660	Accept	1
14	46.152.93.0-46.152.93.255	540-1500	121.187.51.2-121.187.51.255	400-1900	Deny	3
15	Any	Any	Any	Any	Deny	8

The conflict relationship detected by audit system is as follows:

TABLE III. DETECTION RESULTS OF RULE ANORMALIES

Anormaly Type	Rule index													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Shield anormaly			1						8				12	
redundancy anormaly		1								8				
intersection anormaly								10	10					

After the optimization, the rules are gathered as follows:

TABLE IV. THE RULES SET AFTER OPTIMIZATION

Order	S_ip	S-port	D_ip	D_port	Action	Time
1	187.187.0.48-187.187.0.54	680-1280	121.10.7.58-121.12.7.60	220-800	Deny	5
2	187.187.0.44-187.187.255.255	680-1280	121.10.7.0 -121.10.7.255	12 -56	Accept	9
3	152.7.57.0-152.7.57.255	120-655	187.187.0.48	0-680	Deny	5
4	152.57.186.0-152.57.186.255	40-60	121.128.0.0-121.128.255.255	60-560	Accept	12
5	206.220.0.48-206.220.255.255	0-220	121.187.0.45-121.187.0.255	20-80	Accept	3
6	46.152.93.0-46.152.93.255	100-655	121.187.57.0-121.187.57.255	24-120	Accept	8
7	46.152.93.0-46.152.93.255	540-1500	121.187.51.2-121.187.51.255	400-1900	Deny	3
8	Any	Any	Any	Any	Deny	1

VI. CONCLUSION

After the system design is finished, the validity of the experiment is verified by simulation experiments. Experiments use 15 rules of the policy repository for audit which have 3 shield anormalies, 2 intersection anormalies, 2 redundancy anormalies. After the audit system analysis, these anormalies are all found and properly handled. Before the auditing,the average times of rules matching is 4.624, and this number is changed to 3.544 after the audit, so it is proved that the efficiency of the firewall has been significantly improved.

This project presents a method of firewall policy collection and strategy standardization. and provides a method for the automatic audit of firewall which can strengthen the management of the firewall policy configuration and avoid the establishment of security risk strategy. The system has been verified by practice and has received good results.

REFERENCE

[1] Gouda M,Liu Xiangyang. Firewall Design :Consistency, Completeness, and Compactness[C]//Proceedings of the 24th IEEE International Conference on Distributed Computing Systems. [S.1.]:IEEE Press,2004-03.

[2] Fu He Gang,ZHANG Li,. Firewall optimization method based on default rules[J].Computer Engineering,2011,37(20) : 103-104.

[3] ZHUANG Guan Xia. Research and implementation of firewall rule conflict detection and sequence optimization [D].Shanghai: East China Normal University,2011.

[4] HU Wei,DUAN Jin Rong,FAN Min. Research on dynamic filtering rule optimization based on statistical analysis [J]. Information security,2008,24(2):102-103.

[5] Wool A. A Quantitative Study of Firewall Configuration Errors[J]. IEEE computer society, 2004, 37(6): 62-67.

[6] Hamed H, Al-Shaer E. Dynamic rule-ordering optimization for high-speed firewall filtering[C]//Proceedings of the 2006 ACM Symposium on Information, computer and communications security.ACM, 2006: 332-342.

[7] D.Wang,R.Hao,D.Lee. Fault detection in rule-based software systems[J].Information and Software Technology,2012,45(12):865-871.

[8] Hu, H., Ahn, G.L., Kulkarn, K.: Detecting and resolving firewall policy anomalies. IEEE Trans. Dependable Secure Comput.2012, 9(3), 318–331

[9] BenYoussef, N., Bouhoula, A.: Automatic conformance verification of distributed firewalls to security requirements. In: Proceedings of the 2010 IEEE Second International Conference on Social Computing, SOCIALCOM '10, pp. 834–841

[10]Garcia-Alfaro, J., Cuppens, F., Cuppens-Boulahia, N., Preda, S.: Mirage: a management tool for the analysis and deployment of network security policies. In: Proceedings of the 5th International Workshop on Data Privacy Management, and 3rd International Conference on Autonomous Spontaneous Security, 2011.pp. 203–215

[11]Thanasegaran, S., Yin, Y., Tateiwa, Y., Katayama, Y., Takahashi, N.: A topological approach to detect conflicts in firewall policies. In: Proceedings of the IEEE International Symposium on Parallel Distributed Processing, IPDPS 2009, pp. 1–7

[12] Gu Z, Li Y (2011) Research of security event correlation based on attribute similarity. JDCTA Int J Digit Content Technol Appl 5(6):222–228

[13] Kang D, Na J (2012) A rule based event correlation approach for physical and logical security convergence. IJCSNS 12(1):28

[14] Salah K, Elbadawi K, Boutaba R (2012) Performance modeling and analysis of network firewalls. IEEE Trans Netw Serv Manag 9(1):12–21

[15] Krueger T, Gehl C, Rieck K, Laskov P (2010) TokDoc: a self-healing web application firewall. In: ACM symposium on applied computing, SAC 2010, pp 1846–1853

[16] Muraleedharan N, Parmar A (2010) ADRISYA: a flow based anomaly detection system for slow and fast scan. Int J Netw Security Appl 234–245

[17] Nurika O, Aminz M, Rahman ASBA, Zakaria MNB et al (2012) Review of various firewall deployment models. In: 2012 International conference on computer and information science (ICCIS), vol 2. IEEE, New York, pp 825–829.