Audit and Processing of Anomaly Firewall Rules

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

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

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

Abstract—1. Objective: 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 anomaly 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 anomalies in the experimental rule set are all discovered, and the average matching times is reduced from 4.624 to 3.544.

Keywords- Firewall; rule set; anomaly; 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 anomalies. 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: protocol, source address, source port, destination address, destination port, action[2], which is shown in Table I:

<table>
<thead>
<tr>
<th>Firewall rules structure</th>
<th>Field name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Index</td>
<td>i=1,2,3,..n</td>
</tr>
<tr>
<td>2</td>
<td>Protocol</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>3</td>
<td>Source Address</td>
<td>0.0.0.0~255.255.255.255</td>
</tr>
<tr>
<td>4</td>
<td>Source port</td>
<td>0.0.0.0~65535</td>
</tr>
<tr>
<td>5</td>
<td>Destination address</td>
<td>0.0.0.0~255.255.255.255</td>
</tr>
<tr>
<td>6</td>
<td>Destination port</td>
<td>0.0.0.0~65535</td>
</tr>
<tr>
<td>7</td>
<td>Action</td>
<td>Accept, Deny</td>
</tr>
</tbody>
</table>

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 $S_x$ is a set that the rule $R_x$ matched, and $\text{Before} S_x$ is a set that any rule before $R_x$, then
\[
\text{In}_Sx = S_x \cap \text{Before} S_x,
\]
\[
\text{Com}_\text{Before} S_x = \text{Before} S_x - \text{In}_Sx,
\]
\[
\text{Com}_Sx = S_x - \text{In}_Sx
\]
In the above formula $\text{In}_Sx$ is the intersection of $S_x$ and $\text{Before} S_x$, $\text{Com}_Sx$ is the complement of $S_x$ to $\text{In}_Sx$, $\text{Com}_\text{Before} S_x$ is the Complement of $\text{Before} S_x$ to $\text{In}_Sx$. Then these five relationship can be expressed as the following:

- **Contain**: $\text{In}_S r \neq 0$ and $\text{Com}_\text{Before} S r = 0$ and $\text{Com}_S r = 0$.
- **Included**: $\text{In}_S r \neq 0$ and $\text{Com}_\text{Before} S r \neq 0$ and $\text{Com}_S r = 0$.
- **Separate**: $\text{In}_S r = 0$.
- **Intersect**: $\text{In}_S r \neq 0$ and $\text{Com}_\text{Before} S r \neq 0$ and $\text{Com}_S r \neq 0$.
- **Equal**: $S r = \text{Before} S r$.

III. ANORMALY RULES ANALYSIS

Essentially, anomaly 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 anomalies at regular kind by analyzing the relationship between the two rules.

A. **Shield anomaly**

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 anomaly**

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 $\text{r.action} \neq \text{s.action}$ is established, then the rule $r$ and $s$ are intersection anomaly.

C. **Redundancy anomaly**

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: $\text{src_ip}$, $\text{dest_ip}$, $\text{src_port}$, $\text{dest_port}$ and protocol[9]. The $\text{src_port}$ and $\text{dest_port}$ 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 $r_1, r_2, ..., r_n$, and each rule's filtering domain $\text{<protocol src_ip, src_port, dest_ip, dest_port>}$ denoted as $F_1, F_2, ..., F_m$.

Take rule $r_i$ and $r_j$ as an example: Step1: Comparing the protocol domain $F_1$ each belong to $r_i$ and $r_j$, 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 same set of $r_j[F_1]$;
4) $r_i[F_1]$ is not related to $r_j[F_1]$;

Step2: Comparing $r_i[F_2]$ and $r_j[F_2]$ in branch 1, 2, 3. 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](image)
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 anomaly rule is often a minority in rule set, so it is very inefficient to detect each rule for anomalies. 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 anomalies 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 ri’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 ri’s source port with the each node of the standard policy tree to find the node corresponding to the range ri belongs. It will list the results of the risks which are the matched risk nodes which may have caused.

4) ri 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 carried 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:
The following figure is the system control interface:

![Firewall audit system control interface](image-url)
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>
<thead>
<tr>
<th>Order</th>
<th>S_ip</th>
<th>S-port</th>
<th>D_ip</th>
<th>D_port</th>
<th>Action</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>120.655</td>
<td>187.187.0.048</td>
<td>220-800</td>
<td>Accept</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>150-450</td>
<td>187.187.0.34-187.187.0.34</td>
<td>220-800</td>
<td>Accept</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>30-90</td>
<td>187.187.0.35</td>
<td>220-800</td>
<td>Deny</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>40-360</td>
<td>187.187.0.0-187.187.0.255</td>
<td>50-300</td>
<td>Deny</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>40-60</td>
<td>121.128.0.0-121.128.255.255</td>
<td>60-560</td>
<td>Accept</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0-220</td>
<td>121.187.0.45-121.187.0.255</td>
<td>20-80</td>
<td>Accept</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>680-1280</td>
<td>121.10.7.0-121.10.7.255</td>
<td>12-56</td>
<td>Accept</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>680-1280</td>
<td>121.10.7.58-121.12.7.60</td>
<td>220-800</td>
<td>Deny</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>100-700</td>
<td>121.10.7.58-121.12.7.60</td>
<td>22-400</td>
<td>Deny</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>200-500</td>
<td>121.10.7-59.121.12.7.66</td>
<td>40-550</td>
<td>Accept</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>100-655</td>
<td>121.187.57.0-121.187.57.255</td>
<td>24-120</td>
<td>Accept</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>100-405</td>
<td>121.10.7.0-121.12.7.255</td>
<td>15-500</td>
<td>Deny</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>100-200</td>
<td>121.10.7.58-121.12.7.60</td>
<td>90-660</td>
<td>Accept</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>540-1500</td>
<td>121.187.51.2-121.187.51.255</td>
<td>400-1900</td>
<td>Deny</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>8</td>
</tr>
</tbody>
</table>

The conflict relationship detected by audit system is as follows:

<table>
<thead>
<tr>
<th>Anomaly Type</th>
<th>Rule index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shield anomaly</td>
<td>1</td>
</tr>
<tr>
<td>redundancy anomaly</td>
<td>8</td>
</tr>
<tr>
<td>intersection anomaly</td>
<td>10</td>
</tr>
</tbody>
</table>

After the optimization, the rules are gathered as follows:

<table>
<thead>
<tr>
<th>Order</th>
<th>S_ip</th>
<th>S-port</th>
<th>D_ip</th>
<th>D_port</th>
<th>Action</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>680-1280</td>
<td>121.10.7.58-121.12.7.60</td>
<td>220-800</td>
<td>Deny</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>120-655</td>
<td>187.187.0.48</td>
<td>0-680</td>
<td>Deny</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>120-655</td>
<td>187.187.0.48</td>
<td>12-56</td>
<td>Accept</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>40-60</td>
<td>121.128.0.0-121.128.255.255</td>
<td>60-560</td>
<td>Accept</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0-220</td>
<td>121.187.0.45-121.187.0.255</td>
<td>20-80</td>
<td>Accept</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>100-655</td>
<td>121.187.57.0-121.187.57.255</td>
<td>24-120</td>
<td>Accept</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>540-1500</td>
<td>121.187.51.2-121.187.51.255</td>
<td>400-1900</td>
<td>Deny</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
<td>1</td>
</tr>
</tbody>
</table>

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 anomalies, 2 intersection anomalies, 2 redundancy anomalies. After the audit system analysis, these anomalies 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


