Classification and Discovery on Intra-Firewall Policy Anomalies

Lae Win Thwin, Zin May Aye
Department of Computer Technology, University of Computer Studies, Yangon
lewinthwin@gmail.com, zinmay110@gmail.com

ABSTRACT

Firewalls are core elements in network security. However, managing firewall rules is an error-prone task especially for less experience administrator. The reason is that firewall filtering rules itself might cause network vulnerability due to the firewall policy anomalies unless carefully written and ordered them. Thus, firewall rule analysis is essential to determine the proper rule placement and ordering without any policy anomalies when inserting or modifying filtering rules. In this thesis, we develop a firewall rules analyzer based on Intra-Firewall Policy Anomaly Algorithm in order to discover and alert all possible policy anomalies in IPCOP firewall that is used in Small Office Home Office (SOHO) network. And the main purpose of this analyzer is to assist the administrators who setting their firewall to be able to configure conflict-free firewall rules easily by giving advising alerts. We implemented the firewall in a small campus network prototype and experimented it in a virtual network that is built by using Virtual Machine Software (VMWare) Workstation 10. Firewall policy for this system is based on our own predefined security policy for this network. We will test the system that how the developed analyzer can assist the administrators by comparing of the administrator's ability for firewall setting with the help of the analyzer and those without the help of it.

Keywords: *Firewall, ACL, Rules, Anomaly, Firewall Policy*

1. Introduction

Firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewall is a first line of defense of a network. It acts as a barrier between trusted network and untrusted network. It can deploy at the perimeter of the desired network. It can be software or hardware system that prevents unauthorized access from or to a trusted network. It can be implemented one of the system or a combination of both systems. Firewall that permit or deny network traffic based on a firewall policy. Firewall can be used to protect unauthorized users from the external network but also internal users that they are using Internet access with some restrictions. Firewall Policy contains a list of ordered rules that specifies what types of packets should be allowed from/into the protected network. There are five basic types of firewall. They are packet filtering firewall, circuit-level gateways, application level gateways, packet inspection firewalls and multilayer inspection firewalls. In this thesis, we used packet filtering firewall type. Filtering rules consist of filtering fields and an action field. Filtering fields consist of rule order, protocol, source IP address, source port, destination IP address and destination port. Action field consists only action that values can be either accept or deny. Firewall classification means that it checks the conflict among rules in order to avoid firewall policy anomaly. Firewall policy anomaly means that the existence of two or more filtering rules that may match the same packet or the existence of a rule that can never match any packet on the network paths that cross the firewall.

1.1 Related Works

The related work intersects in discovery of firewall policy anomalies, and distributed firewall policy management. Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni [1] first presented for “A Firewall Anomaly Management Policy” in 2010. This paper represents an innovative anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. In particular, a grid-based representation technique was articulated for providing an intuitive cognitive sense about policy anomaly and facilitating efficient policy anomaly management. In addition, the feasibility and applicability of framework was demonstrated through a proof-of-concept prototype of a visualization-based firewall policy analysis tool called Firewall Anomaly

Management Environment (FAME). Alex X. Liu and Mohamed G. Gouda [3] second presented for "Complete Redundancy Detection in Firewalls", in 2005.They made two major contributions in this paper. First, they gave a necessary and sufficient condition for identifying all redundant rules, based on which they categorized redundant rules into upward redundant rules and downward redundant rules. Second, they presented methods for detecting the two types of redundant rules respectively. Their methods made use of a tree representation of firewalls, which is called firewall decision trees. Muhammad Abedin, Syeda Nessa, Latifur Khan, and Bhavani Thuraisingham [2] represented for "Detection and Resolution of Anomalies" in 2006.They discussed some necessary modifications to the existing definitions of the relations. They presented a new algorithm that will simultaneously detect and resolve any anomaly present in the policy rules by necessary reorder and split operations to generate a new anomaly free rule set. They also presented proof of correctness of the algorithm. Then they presented an algorithm to merge rules where possible in order to reduce the number of rules and hence increase efficiency of the firewall.

1.2 Motivation

Firewall is a network security device that monitors incoming and outgoing network traffic. Firewall decides whether to allow or block specific traffic based on its policies. Firewall policies include a set of predefined rules for the entire network or part of network. Firewall policies have become misconfigurations because of the insufficient experiences of administrators. If firewall has thousands of rules, the administrator cannot manage the rule sets. So, this can create network with anomalies free firewall rulesets by using Intra-firewall policy discovery algorithm.

2. Background Theory

Firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewall that permit or deny network traffic based on a firewall policy. In firewall, rule order is important because of the packet filtering process is performed by sequentially matching the packet against filtering rules until a match is found. If the relative rule ordering is not carefully assigned, some rules may be always screened by other rules producing an incorrect policy. When the policy contains a large number of filtering rules, the possibility of writing conflicting or redundant rules is relatively high. Rule conflict classification is essential in intra firewall configuration so that the rulesets should be examined for the presence of rule anomaly such as correlated, shadowed, generalization, irrelevant and redundant anomaly and those conflicts should be eliminated if found. To apply firewall policy, a set of rules are used to assign different partition of the desired network. The number of a set of rules are also known as access control lists (ACLs). In the ACLs, the order of the rule is important. If the first matching rule is found, the remaining rules will also be ignored. So, network administrator need to assign carefully access control rules to correct the requirement of security policy. If the network administrator cannot assign these rules carefully, the firewall policy anomalies can cause in the system.

2.1 Classification of Firewall Anomalies

Firewall policy anomalies were first classified by Al-Shaer et al. [4]. Firewall policy anomalies arise due to the conflicts between the firewall rules when a packet matches more than one rule. Firewall anomalies not only give rise to incorrect packet filtering, but also wastes the available space for storing access control lists (ACL). As already discussed, access control lists (ACLs) of security devices scan rules sequentially; more number of anomalies implies more inconsistent rules which increases the processing time to scan through the rules to match a packet. According to the network environment architecture, firewall policy anomalies can be classified into two types: Intra-Firewall Anomalies and Inter-Firewall Anomalies. In generally, Intra-Firewall Anomalies can occur within one networking device. Another anomaly, Inter-Firewall Anomalies can occur different networking devices.

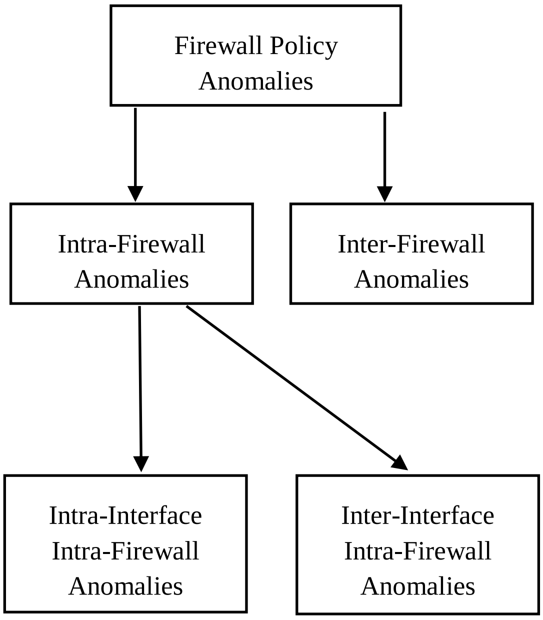
Firewall Policy Anomalies
Intra-Firewall Anomalies
Inter-Firewall Anomalies
Intra-Interface Intra-Firewall Anomalies
Inter-Interface Intra-Firewall Anomalies

Figure 2.1. Classification of Firewall Anomalies

2.1.1 Intra-Firewall Anomalies

Intra-Firewall Anomalies are the conflicts between the rules of the same security device. In other words, when the same packet match two or more rules within the same firewall, an intra-firewall anomaly is said to be present. In practice, security devices like routers, firewalls, layer 3 switch have multiple interfaces. Intra-firewall anomalies can also be categorized into intra-interface intra-firewall anomalies and inter-interface intra-firewall anomalies.

2.1.1.1 Intra-Interface Intra-Firewall Anomalies

Intra-Interface Intra-Firewall anomalies arise due to conflicts between the rules defined in the same interface, typically within one ACL; or in certain cases the anomaly can be between rules of different ACL's, but allocated to the same interface.

2.1.1.2 Inter-Interface Intra-Firewall Anomalies

Inter-Interface Intra-Firewall anomalies arise due to conflicts between the rules defined in different ACL's allocated to different interfaces of the same device. These anomalies occur when the ACL of one interface allows an incoming packet, but the ACL defined on the other interface through which the packet is supposed to pass is denying it or vice versa.

2.1.2 Inter-Firewall Anomalies

Inter-Firewall Anomalies are the conflicts between the rules of two or more devices in the same network. Inter-Firewall anomaly arise when one device permits a packet while other device in its path to destination denies it (as per the security policy defined for the device). Inter-Firewall Anomalies can be between two adjacent devices (within one subnetwork) or between the devices located in different subnetworks.

2.2 Types of Firewall Anomalies

Firewall anomalies can be classified into five anomalies. These are Correlation, Generalization, Redundant, Shadowed and Irrelevant anomalies. For all types of anomalies to discover firewall anomalies, the fields are used in generally. These fields are rule order, source IP address, source port, destination IP address, destination port, protocol and action fields.

2.2.1 Correlation Anomaly

Two rules are correlated if the first rule in order matches some packets that match the second rule and the second rule matches some packets that match the first rule. Rule R_x and rule R_y have a correlation anomaly if R_x and R_y are correlated, and the actions of R_x and R_y are different. If the order of the two rules is reversed, the effect of the resulting policy will be different. Correlation is considered an anomaly warning because the correlated rules imply an action that is not explicitly handled by the filtering rules. Therefore, in order to resolve this conflict, we point out the correlation between the rules and prompt the user to choose the proper order that complies with the security policy requirements.

2.2.2 Generalization Anomaly

A rule is a generalization of another rule if this general rule can match all the packets that match a specific rule that precedes it. Rule R_y is a generalization of rule R_x if R_y follows R_x in the order, and R_y is a superset match of R_x, and the actions of R_y and R_x are different. If the order of the two rules is reversed, the effect of the resulting policy will be changed. Therefore, as a general guideline, if there is an inclusive match relationship between two rules, the superset (or general) rule should come after the subset (or specific) rule. Generalization is considered only an anomaly warning because the specific rule makes an exception of the general rule, and thus it is important to highlight its action to the administrator for confirmation.

2.2.3 Redundant Anomaly

A redundant rule performs the same action on the same packets as another rule such that if the redundant rule is removed, the security policy will not be affected. Rule R_y is redundant to rule R_x if R_x precedes R_y in the order, and R_y is a subset or exact match of R_x, and the actions of R_x and R_y is similar. If R_x precedes R_y in the order, and R_x is a subset match of R_y, and the actions of R_x and R_y are similar, then Rule R_x is redundant to rule R_y provided that R_x is not involved in any generalization or correlation anomalies with other rules preceding R_y. If the redundant rules are removed, the effect of the resulting policy will not be changed. Redundancy is considered an error. A redundant rule may not contribute in making the filtering decision, however, it adds to the size of the filtering rule table, and might increase the search time and space requirements. It is important to discover redundant rules so that the administrator may modify its filtering action or remove it altogether.

2.2.4 Shadowed Anomaly

A rule is shadowed when a previous rule matches all the packets that match this rule, such that the shadowed rule will never be activated. Rule R_y is shadowed by rule R_x if R_y follows R_x in the order, and R_y is a subset match of R_x, and the actions of R_x and R_y are different. If the second rule is shadowed with the first rule, the second rule will never get activated. Shadowing is a critical error in the policy, as the shadowed rule never takes effect. This might cause a permitted traffic to be blocked and vice versa. It is important to discover shadowed rules and alert the administrator who might correct this error by reordering or removing the shadowed rule.

2.2.5 Irrelevant Anomaly

A filtering rule in a firewall is irrelevant if this rule cannot match any traffic that might flow through this firewall. This exists when both the source address and the destination address fields of the rule do not match any domain reachable through this firewall. If there is more number of irrelevant anomalies implies more inconsistent rules which increases the time to scan through the rules to match a packet. Thus, this rule has no effect on the filtering outcome of this firewall. It is also only anomaly warning and thus it also advises to the administrator for confirmation.

3. Firewall Anomalies Classification and Discovery

Firewall uses to filter incoming and outgoing network traffic. Firewall can also be classified into two types: software firewall and hardware firewall (network firewall). Software firewall uses in this paper. There are many software firewalls such as pfSense, IPFire, OPNsense, Zeroshell, IPCop firewall, etc. Among them, we use IPCop Firewall to test firewall rules because this is used for SOHO network, open source and easy to use. This firewall is implemented in the VMware Workstations to define security policy, network interfaces and access control rules. To discover firewall anomalies, we used Intra-Firewall Anomaly Discovery Algorithm in this thesis.

3.1 Intra-Firewall Anomaly Discovery Algorithm

Intra-Firewall Anomaly Discovery Algorithm is used in the system to detect anomalies.

```
Algorithm 1: DetectIntraAnomalies (All ACL)
Input: All Access Control Lists
Output: Shows the Intra-firewall policy anomalies
for each acl ∈ All ACL
   If currentIP ≡ acl.ip
     Then currentACL[i] ← acl
       i ← i+1
       j ← 1
         for each currentACL
           for k ← j to i
             do DetectAnomaly(k,currentACL,acl)
           j ← j+1
       currentIP ← acl.ip
       index ← findIndex(acl.ip)
       InterACL ← AllACL.ip ∈index
       for i ← 0 to len(InterACL)
          do DetectAnomaly(i,InterACL,acl)
       currentACL.clear()
       i ← 0
```

```
Algorithm 2: DetectAnomaly(index,acl1,acl2)
Input: Two Access Control Lists
Output: If the ACL's are conflicting, return its anomaly type.
if $(acl1.prot \subseteq acl2.prot \wedge acl1.src \subseteq acl2.src \wedge acl1.dest \subseteq acl2.dest \wedge acl1.action = acl2.action) \vee (acl1.prot \supseteq acl2.prot \wedge (acl1.src \subseteq acl2.src \vee acl1.src \supset acl2.src) \wedge (acl1.dest \subseteq acl2.dest \vee acl1.dest \supset acl2.dest) \wedge acl1.action = acl2.action)$
    then anomaly $\leftarrow$ Redundant
        return (anomaly)
if $(acl1.prot \subseteq acl2.prot \wedge acl1.src \subseteq acl2.src \wedge acl1.dest \subseteq acl2.dest \wedge acl1.action \neq acl2.action)$
    then anomaly $\leftarrow$ Shadowed
        return (anomaly)
if $(acl1.prot \subseteq acl2.prot \wedge acl1.src \subseteq acl2.src \wedge (acl1.dest \subseteq acl2.dest \vee acl1.dest \supset acl2.dest)) \vee (acl1.prot \subseteq acl2.prot \wedge acl1.src \supseteq acl2.src \wedge (acl1.dest \subseteq acl2.dest \vee acl1.dest \supset acl2.dest))$
    then anomaly $\leftarrow$ Correlation
        return (anomaly)
if $(acl1.prot \supseteq acl2.prot \wedge acl1.src \supseteq acl2.src \wedge acl1.dest \supseteq acl2.dest \wedge acl1.action \neq acl2.action)$
    then anomaly $\leftarrow$ Generalization
        return (anomaly)
```

The following explanation is the detail explanation of Intra-Firewall Anomaly Discovery Algorithm. In the Intra-Firewall Anomaly Discovery Algorithm, there are examined with many fields. In this algorithm, firstly it examines protocol filed. Second, it also examines source IP address and then destination IP address. Finally, it examines action field. In the field of protocol, source IP address and destination IP address, the examination of these three field can be examined with four conditions. These are equal, subset, superset and not equal. But the action field can be examined only two conditions. These can accept or deny action. In this algorithm, we examined step by step for each rule. Finally, the algorithm outputs four results that are anomalies. These results are shadowed anomaly, redundant anomaly, general anomaly and correlation anomaly. This algorithm is also named as Firewall Policy Advisor Analyzer. There are five types of firewall anomalies. But in the system this algorithm is used, so the output will be only four types of anomalies rather than all five types of anomalies.

3.2 IPCop Firewall

In this system, IPCop firewall is used to assign security policy and to discover firewall anomalies. IPCop is an Open Source Linux Firewall Distribution project. Its main goal is to provide a secure and stable Firewall, which is easy to configure and maintain. IPCop has a web interface and it provides easy upgrade and patch management.

3.2.1 Network Interfaces of IPCop Firewall

IPCop firewall has four network interfaces to create network architecture. These are RED, ORANGE, GREEN and BLUE interfaces. RED interface refers to insecure public network such as the internet. ORANGE interface refers to Demilitarized Zone (DMZ) network such as separate network from the internal network. This network is a special local network configuration used to improve internal private network security by separating computers on each side of a firewall. GREEN interface refers to secure private network such as local area network. BLUE interface refers to the access point such as wireless network.

3.2.2 Rule Interfaces of IPCop Firewall

IPCop firewall has five interfaces to define access control rules. These are Outgoing Traffic, IPCop Access, Internal Traffic, Port Forwarding and External IPCop Access. Outgoing traffic is the traffic from the local network interface such as orange network or green network to the insecure network interface such as the Internet. IPCop access is the traffic from the local network interface such as green network or orange network to the IPCop firewall. Internal traffic is the traffic between orange network interface and green network interface. Port Forwarding is the traffic from insecure network such as red interface to local area network interface such as green interface or orange interface. The remaining interface, external IPCop access is the traffic from the red interface to the IPCop firewall.

3.2.3 Default Settings of IPCop Firewall

The default settings of IPCop Firewall is mentioned in the following. The traffic from GREEN interface to other interfaces that are ORANGE interface, RED interface and BLUE interfaces are not allowed. The traffic from ORANGE interface is only allowed to RED interface but other interfaces that are GREEN interface and BLUE interface are blocked. The traffic from BLUE interface to other interfaces that are GREEN interface, ORANGE interface and RED interface are also blocked. The traffic from RED interface to other interfaces that are GREEN interface, BLUE interface and ORANGE interface are also blocked.

4. System Design and Implementation

In this paper, network architecture is implemented by using VMware Workstation. The version of VMware Workstation 10 is used in the system. VMware Workstations is a virtual machine software which can be used for computer to run multiple operating system over a single physical host computer. Each virtual machine can run a single instance of any operating system (Window, Linux, etc.) simultaneously. VMware workstation strongly supports hardware compatibility and works as a bridge between the host and virtual machine for all kinds of hardware resources.

4.1 System Architecture

The system architecture is considered base on the general environment. Firewall rules are assigned according to security policy by using IPCop firewall. In IPCop firewall, three network interfaces are only assigned in VMware Workstations. In this system, three network interfaces are assigned which are RED interface, ORANGE interface and GREEN interface with limitation of VMware Workstations. The following figure 4.1 shows the system architecture of the system.

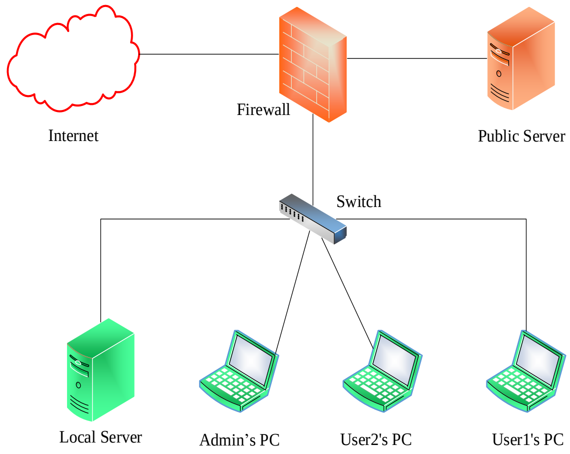

Figure 4.1. Network Topology

The following table shows IP address, gateway and network portions of figure 4.1.

Name	IP address	Gateway	Network
Internet	200.10.50.5	200.10.50.1	RED
Public Server	192.168.108.108	192.168.108.1	ORANGE
Local Server	192.168.49.132	192.168.49.1	GREEN
Admin's PC	192.168.49.131	192.168.49.1	GREEN
User2's PC	192.168.49.130	192.168.49.1	GREEN
User1's PC	192.168.49.129	192.168.49.1	GREEN

Local Server and Public Server are implemented with most useful servers such as WEB Server, DNS Server, SSH Server and FTP Server. To test firewall anomalies, the predefined rules can also be assigned according to the security policy of the system.

4.1.1 Security Policy of the System

The security policy of the system is the following. User1's PC is not allowed to access the Internet. ORANGE network is not allowed to access IPCop Firewall. Only admin PC can access IPCop Firewall. The users from green network are only allowed to access DOMAIN, WEB and PING services to ORANGE network. File service is not allowed to access in it. External users are allowed to access WEB, PING and FTP services to ORANGE network. External users are not allowed to access WEB, PING and SSH services to IPCop Firewall.

4.1.2 Predefined Rules

According to the security policy, 34 predefined rules are defined in the system. These rules are only for sampling to test anomalies. The predefined rules can be varied according to the security policy and environment's requirements. In practice, IPCop firewall has five interfaces to assign firewall rules. The rules are assigned to these five interfaces according to the traffic. There are **two** rules in Outgoing Traffic, **fourteen** rules in IPCop Access, **ten** rules in Internal Traffic, **four** rules in Port Forwarding and **four** rules in External IPCop Access.

4.2 Implementation of the System

There are two parts to implement of the system. The first part is system environment setup and the second is program setup. In the system environment setup, VMWare Workstations 10 is used to create logical network topology. To create logical network topology, user needs to install VMWare Workstations 10 in user's PC. In VMWare, firstly, **one** virtual machine is used to install IPCop firewall in it. In IPCop firewall, user needs to setup network portions that are RED, ORANGE and GREEN network. In this logical topology, there are **four** virtual machines for GREEN network, **one** virtual machine for ORANGE network and **one** virtual machine for RED network. Finally, the created virtual machines are assigned with IP address and default gateway. The second part is program setup. In the program setup, there are four steps to test firewall anomalies. The first step is to save the predefined rules of IPCop Firewall as html file and the second is input this saved html file to the Firewall Policy Advisor Analyzer. This analyzer is used the process of Intra-Firewall Policy Anomaly Discovery Algorithm. The third is import file to check the rules lists and finally check the rules to output the generalization anomalies, shadowed anomalies, correlation anomalies and redundant anomalies. The following figure 4.2 shows the flowchart of the implemented system.

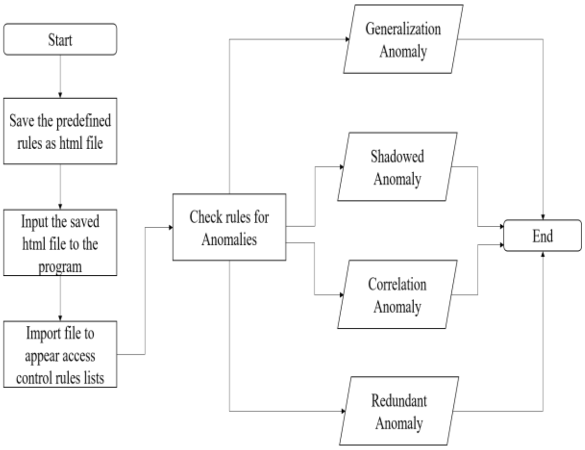
Start
Save the predefined rules as html file
Input the saved html file to the program
Import file to appear access control rules lists
Check rules for Anomalies
Generalization Anomaly
Shadowed Anomaly
Correlation Anomaly
Redundant Anomaly
End

Figure 4.2. Flowchart of the Implemented System

4.3 Result and Discussion

IPCop firewall is used to secure local private network with filtering rules. If administrator is less experience or the filtering rules have hundred or thousand that are not order correctly, the result become incorrect. Administrator or user needs to apply the program which act as Analyzer for Firewall Policy Advising in this system. The algorithm of the Analyzer is mentioned in Figure 4.2. After implementing predefined rules with this analyzer, it advises administrator or user four types of anomalies. Administrator or user also need to check these anomalies which are needed to remove or change the order in the rules lists to correct the output result.

5. Conclusions and Further Works

Although firewall is the most powerful security devices in network, its configuration of policy anomalies might be the main reason of causing firewall itself vulnerabilities. Administrators with less experiences have more possibility to configure these anomalies when their system is larger and more complex. Therefore, firewall policy analyzer is developed based on VMware workstations in this system for administrators in order to use as an assistant when they configure their firewall policy setting. This system outputs with table format of the anomalies. This system will reduce firewall rule conflictions configured by administrators by alerting all possible types of firewall anomalies depending on their rule order.

5.1 Limitation of the System

Limitation of the system is implemented in VMware workstations. In VMware workstations, only five virtual machines are opened in simultaneously. So, the predefined rules can only define by using these five machines. In reality, we can define with many rules. This is the limitation of VMware workstations. Another limitation is IPCop feature with VMware workstations. In IPCop firewall, only define three interfaces are defined rather than four interfaces in virtual machines. If the test with real device, it can assign for BLUE network that is used for wireless users. But this interface cannot assign with multiple access control rules. This interface can only assign two conditions for outgoing traffic. These two conditions are accepted or not to other interfaces. The default condition is blocked to all other interfaces.

The future work includes practical implementation of inter- and intra-firewall management tool in real-time environment. Also, the ability to handle inconsistencies in distributed networks is also left as a part of future work.

References

[1] Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "A Firewall Anomaly Management Policy," Arizona State University, USA, 2010

[2] Muhammad Abedin, Syeda Nessa, Latifur Khan, and Bhavani Thuraisingham, "Detection and Resolution of Anomalies," Department Of Computer Science, The University of Texas at Dallas, 2006

[3] Alex X. Liu and Mohamed G. Gouda, "Complete Redundancy Detection in Firewalls," Department of Computer Sciences, The University of Texas at Austin, Austin, Texas 78712-0233, USA, 2005

[4] E. Al-Shaer, "Classification and Discovery of Firewalls Policy Anomalies," Springer International Publishing Switzerland, 2014