Term Paper I

Cloud-Based Firewall Policy Management

Swapnil Hasabe
Computer Science
University of Texas at Dallas
sdh140430@utdallas.edu
CS6301: Securing and Developing Cloud
Instructor: Dr. Bhavani Thuraisingham

ABSTRACT

In this paper, I have discussed about cloud-based firewalls, how firewall policies are managed to provide security to cloud. Cloud-based firewall s fall into two categories: Host based firewalls also known as Software as a Service. Second one is Network based Firewalls policies. This cloud-based firewall deployed in Managed Security Service provider (MSSP). The second point I have focused on is firewall policy configurations. I have discussed some algorithms which help to find out errors in firewall policies. Reason behind discussing these issues is as we are suffering from unintended security loop holes. These security holes become more dangerous when any unauthorized users attack to enterprises to gain benefits in form of money or they may want to make harm to businesses. For ensuring the security of private cloud in most businesses and enterprises, firewalls are mostly deployed in security mechanism. The quality of policy configured in firewall decides how much it would be effective for securing the private networks. As we know, designing firewall policies are often error-prone due to the complexity of firewall configurations as well as the lack of knowledge of administrator. Designing Diverse Firewall policy is the efficient method which can be used to detect function discrepancy between multiple policies.

1. INTRODUCTION: Several years ago, may security and network administrators were worried about lack of best firewall management for cloud environments. But nowadays, better solutions are available for host based firewall management and public cloud based firewall management. In recent years, there is a significant increase in the usage of computers and their capabilities to communicate with each other. It increased the need for more cloud security and firewalls have proved themselves an important factor of providing cloud security. As the policy is made up of rules, the quality of these firewall policies depends on knowledge of administrator. Unfortunately, there is little help for their administrators to understand the actual meaning of the firewall rules. A firewall policy consists of a sequence of rules where each rule is in form of <predicate> → <decision>. The predicate part contains packet fields such as source IP address, destination IP address, source port number, destination port number, and protocol type. The decision of rule can be accept, or discard, or logging option.

2. OVERVIEW: To develop a Diverse Firewall policy, we need three phases: a design phase, a comparison phase, and a resolution phase [1]. Here, two firewall policies in terms of sequence of rules are taken as the input, in design phase, two firewall policies are converted into firewall decision diagram(FDD), in the comparison phase, the resulting firewall policies are compared with each other to detect all functional discrepancies between two given firewall policies. All functional discrepancies are resolved in resolution phase.

3. RELATED WORK: This idea of design diversity is inspired by N-version programming [3]. The basic concept of N-version programming is to give the same requirement specification to N teams to independently design and implement N programs using different algorithms, languages, or methods. Then the resulting N programs are executed in parallel. A decision selection mechanism is applied to examine the N results for each input from the N programs and selects a correct or "best" result. It means we achieved diversity here. The key element of N-version programming is design diversity [1].

4. APPROACHES:

There are three approaches discussed to maintain firewall policy management in the cloud.

4.1. **Host- Based Cloud Firewall management:**

In Infrastructure as a Service (IaaS) environments, there are different brands available in market like McAfee Inc., Symantec Corp. Organizations can simply install one of these agent-based product from vendors. Some of them also provide console based firewall management feature.

4.2. **The second approach** is to detect errors after firewalls have been designed. We concentrate on second approach. In this approach, administrator manually examines every pair of conflicting rules to see whether the two rules need to be edited or a new rule needs to be added. These firewall policies are compared to each other in form of FDDs. In this paper, we take efforts to analyze change-impact of firewall policies because as requirements of private networks changes, configuration of firewall policy needs to be changed [2]. Please refer [1] for all algorithms pseudo code.

4.2.1. Proposed System:

Following are the major components of our system: - Knowledgeable administrator - Firewall Decision Diagram concept - Firewall server Authentication for administrator - Firewall policies.

Administrator configures the firewall policy, so it is very important to keep firewall server authentication. Administrator has to log in before configuring firewall policy in form of rules.

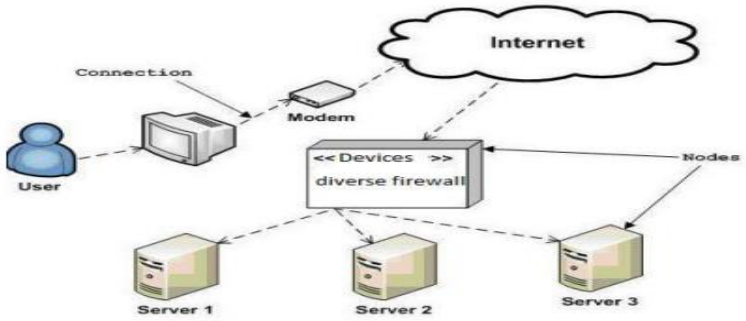


Fig. 1: Deployment of system

4.2.2 Running Example:

Requirement specification for every team:

The mail server with IP address 192.1.2.3 can receive emails. The packets from an outside malicious domain 192.168.0.0/16 should be blocked. Other packets should be accepted and allowed to proceed.

4.2.2.1. Team A constructed Firewall decision diagram according to their firewall policy design.

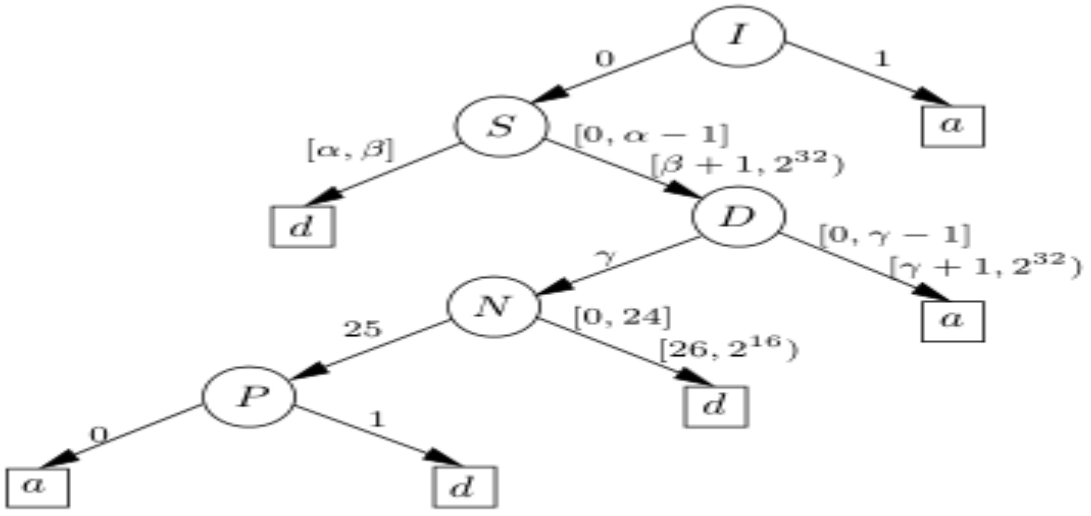


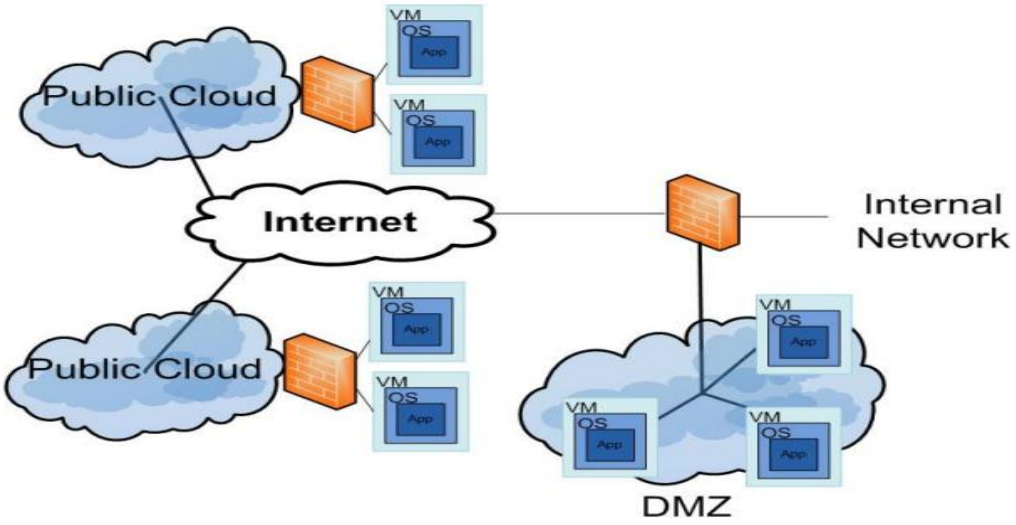
Figure 3. The FDD by Team A

4.2.2.2. Team B constructed firewall policy by their own. It includes three rules.

1. $(I \in \{0\}) \wedge (S \in all) \wedge (D \in \{\gamma\}) \wedge (N \in \{25\}) \wedge (P \in \{0\}) \rightarrow a$
2. $(I \in \{0\}) \wedge (S \in [\alpha, \beta]) \wedge (D \in all) \wedge (N \in all) \wedge (P \in all) \rightarrow d$
3. $(I \in all) \wedge (S \in all) \wedge (D \in all) \wedge (N \in all) \wedge (P \in all) \rightarrow a$

Figure 4. The firewall by Team B

4.3. Public Cloud: Below figure shows that role of firewall rule management in public cloud. In the public cloud, you will find many individual systems which lead to problem of firewall management. Increasing unique rules regarding each firewall policy must be managed. For instance, one might be using Cisco firewalls for private cloud for internal security but it might be possible that public cloud vendor only support check point firewalls policies. So point is public cloud needs to have multiple vendor interfaces. But what if the requirement of organization changes? Administrator also needs to make changes in firewall policies.



5. ANALYSIS:

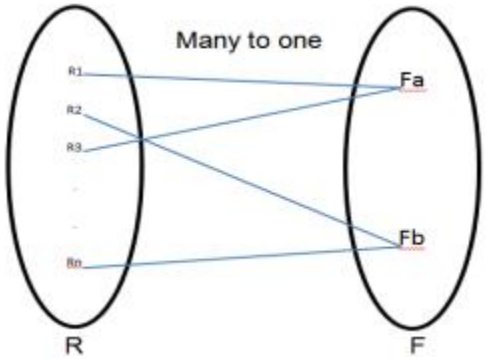
5.1. Mathematical Model for diverse firewall design:

Firewall policy Analysis: one can apply algorithms to figure out the vulnerabilities, conflicts, anomalies and redundancy in given policy.

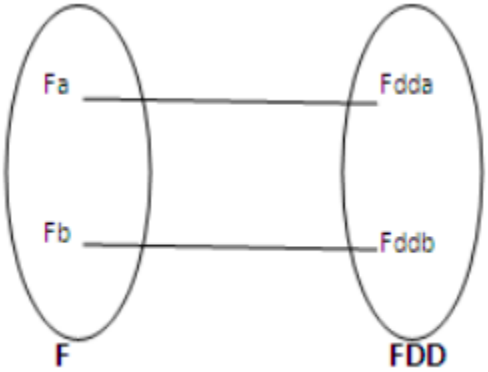
1. Let „S" be the set of diverse firewall design system and representing by S= {R, F, FDD, Fs}.

2. R={R| R is set of all rule in requirement specification }R={ R1, R2, R3, …, Rn}Where R1={r1,r2,r3… rn},R2={r1`,r2`,r3`,…,rn`},R3={r1``,r2``,…,rn``}.. set represents Firewall policy set F = {Fa, Fb,…. , Fn} Where Fa={R1},Fb={R2},Fc={R3}

3. FDD set represents Firewall Decision Diagram for different firewall policy set FDD={Fa`,Fb`,…,Fn`} 4. Fs set represent semi isomorphic equivalent of FDD. Fs={Fa``,Fb``,….,Fn``} C={R,O,F} The process take rules(R) as input and combine to make Firewall Policy(F).



C={F,Fdd} This process take firewall policy as input and convert it into FDD.



D={RD,O,DF} Every discrepancy is discussed and resolved by all teams and finally generates Diverse Firewall.

We are using concept of Firewall Decision Diagram (FDD) to construct firewall policy. We are using algorithms: a construction algorithm [7], a comparison algorithm to detect functional discrepancies. This concept helps to understand how firewall policies are compared to each other to detect all functional discrepancies. Designing firewall policies suffers from three problems: the consistency problem, the completeness problem, and the compactness problem [6].

5.2. Change - Impact analysis:

This solution works when business security requirements are continuously evolving. Suppose, current policy states that firewall should deny the email coming from the source 192.128.123.01. But as requirements might change after some period, so new requirement is above mentioned is found to be authorized. So, administrator has to change policy configuration. He can do it by adding, removing or modifying the rules in policies.

5.3. Advantages and Disadvantages of Cloud based firewall policies:

5.3.1: Scalability: Cloud based firewalls providers deliver cloud services to many customers as like organizations. When bandwidth increases then scalability plays an important role in management.

5.3.2. Availability: It provides solution to the single point of failure. Statistics shows that cloud service provides offers >99.99% availability.

5.3.3 Extensibility: Cloud based firewalls are available everywhere in public cloud.

5.3.4. Lack of security knowledge (CSP)

6. CONCLUSION

To maintain cloud based firewall policy management, administrator needs to change policy rules according to requirement changes. On the other side, single firewall policy can be set once, and no longer need to be updated if we know that there is only change in server's location in cloud. There are many tools and frameworks in the market which provides cloud firewall management automation. The method of diverse firewall policy design is effective in practice and can be used flexibly in a variety of scenarios. Cloud Based firewalls has advantages as well as disadvantages. This paper deals with the method that can compare two firewall policies and detect all functional discrepancies between them in human readable format. This method also can be used in change-impact analysis. In addition, this paper leads to develop solutions for firewall policies verification and policies redundancy checking.

7. REFERENCES

[1]. Alex X. Liu, Member, IEEE, Mohamed G. Gouda, Member, IEEE "Diverse Firewall Design",2008

[2]. Alex X. Liu, Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824-1266, U. S. A., "Change-Impact Analysis of Firewall Policies", 2012

[3]. A. Avizienis, "The Methodology of N-Version Programming," Software Fault Tolerance, Chapter 2, M.R. Lyu, ed. Wiley, pp. 23-46,1995.

[4]. Y. Naveh, Y. Richter, Y. Altshuler, D. L. Gresh, D. P. Connors, Workforce optimization: Identification and assignment of professional workers using constraint programming, IBM J. RES. & DEV. VOL. 51 NO. 3/4 MAY/JULY 2007

[5]. Ada Yetunde Barlatt, Models and Algorithms for Workforce Allocation and Utilization, (Industrial and Operations Engineering) in The University of Michigan, 2009

[6]. M. G. Gouda and A. X. Liu. Firewall design: consistency, completeness and compactness. In Proceedings of the 24th IEEE International Conference on Distributed Computing Systems (ICDCS-04), pages 320– 327, March 2004.

[7]. M. G. Gouda and A. X. Liu. Structured firewall design. Computer Networks Journal (Elsevier), 51(4):1106–1120, March 2007.

[8]. Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ketan Kulkarni, "Detecting and Resolving Firewall Policy Anomalies"

[9] http://www.iosrjen.org/Papers/vol3_issue4%20(part-2)/F03423336

[10]http://searchcloudsecurity.techtarget.com/tip/Enterprise-considerations-for-cloud-firewall-management-and-automation