Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.359 – 367

RESEARCH ARTICLE

Firewall and Its Policies Management

Er. Smriti Salaria[1], Er. Nishi Madaan[2]

[1]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
[2]Department of Computer Science and Engineering, DAV University, Jalandhar, Punjab, India
[1] Smritisalaria@yahoo.in; [2] nishi.02.bti@gmail.com

Abstract: Firewalls are core elements in network security. A firewall element determines whether to accept or discard a packet that passes through it based on its policy. Firewall allows separation between frontend and backend entity so as to ensure security. In this paper we have critically analyzed various firewall management policies and techniques and also have covered our views such that its major types, classification and applications.

Keywords: Firewall; Firewall types; proxy server; Firewall policies; Firewall Policies types

I. INTRODUCTION

A firewall is software or hardware based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. Due to the increasing threat of network attacks, firewall has become more important elements to secure our data from the unauthorized attacks on the network. Its task is ideally to filter out unwanted network traffic coming from or going to the secured network. The filtering decision is based on the firewall policy which is set of ordered filtering rules defined according to predefined security policy requirements. The effectiveness of firewall security is dependent on providing policy management techniques/tools that enables network administrators to analyze, purifying and verify the correctness of written firewall legacy rules.

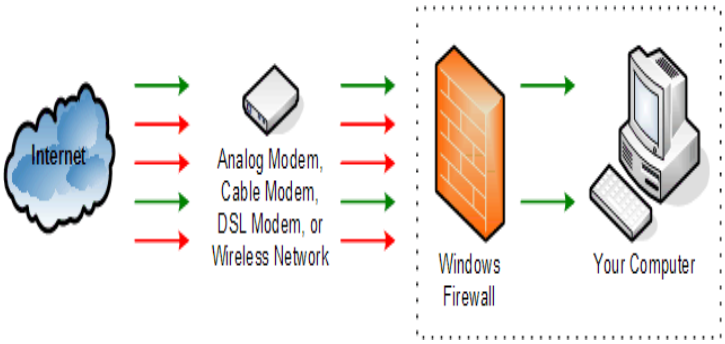

Figure 1: working of Windows Firewall

A. Need of firewall:

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals

- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization

B Types of firewall

Basically there are three types of firewall.
a). Network layer firewall.
b). Application layer firewall.
c).proxy firewall.

a). Network layer firewall:-

Network layer firewalls also called packet filters; operate relatively low level of TCP/IP protocol stack not allowing packets to pass through the firewall unless they match the established rule set. Network layer generally fall into two subcategories stateful and stateless. In stateful , firewall maintain context about active sessions and use that state information to speed packet processing and on the other hand stateless firewall require less memory and can be faster for simple filters that require less time to filter than to look up a session.

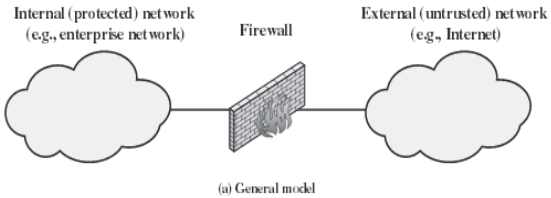

Figure 2: Network Layer Firewall.

b). Application layer firewall:-

Application layer firewall work on the application level of the TCP/IP stack (i.e. all browser traffic, all telnet or all FTP traffic) and may intercept all packets travelling to or from an application. It is used to block the other packets. Application layer filtering goes beyond packet filtering and allows you to be much more granular in your control of what enters or exits the network. While packet filtering can be used to completely disallow a particular type of traffic (for example, FTP), it cannot “pick and choose” between different FTP messages and determine the legitimacy of a particular FTP message.

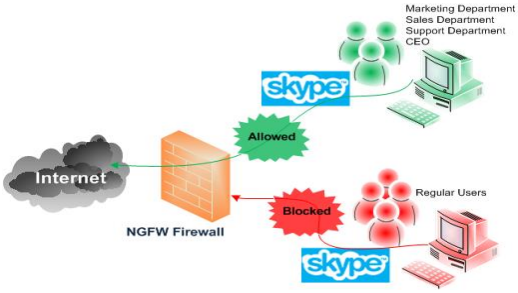

Figure 3: Application Layer Firewall.

c). Proxy firewall filters:-

Proxy firewalls are the most secure types of firewalls, but this comes at the expense of speed and functionality, as they can limit which applications your network can support. The enhanced security of a proxy firewall is because, unlike with other types of firewall, information packets don't pass through a proxy. Instead the proxy acts as an intermediary - computers make a connection to the proxy which then initiates a new network connection based on the request; effectively a mirror of the information transfer. This prevents direct connections and packet transfer between either sides of the firewall, which makes it harder for intruders to discover where the location of the network is from packet information. A firewall proxy provides internet access to computers on a network but is mostly deployed to provide safety or security by controlling the information going in and out of the network. Firewall proxy servers filter, cache, log, and control requests coming from a client to keep the network secure and free of intruders and viruses.

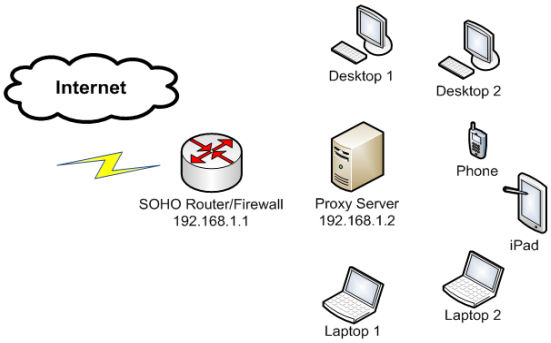

Figure 4: Proxy Server.

II. POLICIES OF FIREWALL MANAGEMENT

A. Firewall policy Modeling

As a basic requirement of any firewall policy management, we first modeled the relations of firewall rules in the policy. We describe formally our model of firewall rules relations and policies.

Formalization of Firewall Rule Relations

To be able to build a useful model for filtering rules, we need to determine all the relations that may relate two or more packet filters. In which we match two values, two values are equals if they matched, inclusive if one values is subset of another, distinct otherwise. Example

Definition 1: Rules Rx and Ry are exactly matched if every field in Rx is equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are exactly matched since all corresponding fields in both rules are equal.

1: tcp, 140.192.37.10, any, 163.122.51.∗, 21, accept
2: tcp, 140.192.37.10, any, 163.122.51.∗, 21, deny

Definition 2: Rules Rx and Ry are inclusively matched if they do not exactly match and if every field in Rx is a subset or equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are inclusively matched since they do not exactly match and every field in rule 1 is a subset or equal to the corresponding field in rule 2. Rule 1 is the subset match of the relation while rule 2 is the superset match.

1: tcp, 140.192.37.10, any, 163.122.51.∗, 80, accept
2: tcp, 140.192.37.∗, any, 163.122.51.∗, any, deny

Definition 3: Rules Rx and Ry are completely disjoint if every field in Rx is not a subset and not a superset and not equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are completely disjoint since all corresponding fields in both rules are distinct.

1: tcp, 140.192.37.10, 2000, 163.122.51.50, 80, accept
2: udp, 140.192.37.20, 3000, 163.122.51.60, 21, accept

Definition 4: Rules Rx and Ry are part subset or a superset or equal to the corresponding field in Ry, and there is at least one field in Rx that is not a subset and not a superset and not equal to the corresponding field in Ry.

For example, rule 1 and rule 2 below are partially disjoint (or partially matched) since all fields in rule 1 are related to the corresponding fields in rule 2 except the destination port field.

1: tcp, 140.192.37.10, any, ∗.∗.∗.∗, 80, accept
2: tcp, 140.192.37.∗, any, ∗.∗.∗.∗, 21, deny

Definition 5 Rules Rx and Ry are correlated if some fields in Rx are subsets or equal to the corresponding fields in Ry, and the rest the fields in Rx are supersets of the corresponding fields in Ry.

For example, Rule 1 and rule 2 below are correlated since they have the same protocol, source and destination ports, and the source address of rule 1 is a subset of the corresponding fields in rule 2 , and the destination address of rule 1 is a superset of that of rule 2.

1: tcp, 140.192.37.10, any, ∗.∗.∗.∗, 80, accept
2: tcp, ∗.∗.∗.∗, any, 140.192.37.∗, 80, deny

B. Firewall policy Anomaly detection

A firewall policy anomaly is defined as the existence if two or more different filtering rules that match the same packets. Here we define different types of anomalies that may exist among filtering rules in a firewall policy.

Firewall policy anomaly types:

1). Shadowing anomaly: A rule is shadowed when a previous rule matches all the packets that matches this rule, such that the rule of shadowed will never be evaluated. Shadowing is a critical error in the policy as the filtering rules never be effects.

2). Correlation anomaly: Two rules are correlated , if they have different filtering actions, if the first rule in order to matches some packets that matches the second rule and the second rule matches some packets that match the first rule.

3). Redundancy anomaly: A rule is redundant if there is another rule that produces the same matching and action such that if the redundant rule is removed, the security policy will not be affected.

4). Generalization anomaly: A rule is a generalization of another rule if the first rule matches all the packets that the second one could match but not the opposite.

C. Automated correction of policy fault

This policy is very useful in firewall management. It has its own difficulties to apply correctly in the firewall. These difficulties can be categories in separate groups:

- Define the type of faults and counting the number of faults.
- Locating the origin of the fault.
- Correcting the faults without making any side effects on other rules.

To resolve these difficulties there are different techniques we use.

- First technique is random packet generation. For using this technique domain of each of policies should be defined and packet will be generated randomly.
- Second technique generates packets based on local constraint solving. It analyzes each rule separately and checks condition.
- Third is packet generation based on global constraint solving. In this technique, overlaps of predicates are considered by analyzing the policy and also the constraints of the policy. It has better efficiency in terms of covering the target entities, but the limitation is the large amount of needed time for analysis.

D. Fault localization

A very important part of the management of firewall policies is to fix the fault, for this first we should define the root of the fault in the debugging phase of testing. Finding of the root of the fault is called fault localization. In which two approaches are used to decrease the cost of debugging and fault localization.

- RDC (Rule Decision Change) shows that the decision is correct or incorrect about a special rule.
- RFC (Rule Field interval Change) shows a false definition of an interval in a rule.

It will take very long time in testing and debugging because of the inherent complexity of fault localization and the huge amount of roots. The number of roots to be inspected is decreased by analyzing the characteristics come from faults in failed test cases. The process of reducing the number of rules to be inspected and ranking them has been categorized in three separate techniques. The first technique is called Covered-rule-fault localization. The idea is useful when there are so many rules that are covered by failed test cases. In this case, it has been suggested to policy testers to give the highest priority to the earliest rule that has been covered. The second technique introduce the way for the case that the earliest placed rule that is addressed by failed test cases has no fault. In this special situation the earliest placed rule is in a higher priority. After selecting rules by the previous technique the third technique will select from them those with more probability to be faulty one. In this technique the idea is that the decision of faulty rules and other rules should be different from each other.

E. Firewall Policy Editor

Firewall policies are often written by different network and occasionally updated (by inserting, modifying or removing rules)to accommodate new security requirements and network topology changes. Editing a security policy can be far more difficult than creating new one. The policy editor helps the user to determine the proper order for a new and modified rule in the policy. We present the editing, modifying and removal process as implemented in our policy editor.

1. *Rule insertion*: The order of new rule in the firewall policy is determined based on its relation with other existing rule. In general a new rule should be inserted before any rule that is a superset match and after any rule that is a subset match of this rule.

2. *Rule removal*: In general, removing a rule has much less impact on the firewall policy than insertion. To remove the rule the user enters the rule number to retrieve the rule from the rule list and select to remove it.

F. Firewall Tools

In managing firewall policies is developing tools which help administrators in dealing with complex and time consuming task. There are various tools used in firewall policies among them policy anomaly is very popular. The anomaly management of firewall policy works, based on a segmentation technique which is rule based.

III. ANOTHER POLICY TYPES

- IP Address Protocols Based Traffic
- Application Specific based Traffic
- Based on the Network Activity
- Based on the User's Identity.

Firewall policy based on the IP Address

Firewalls allow only specified protocols to pass through. These protocols are such as the Internet Protocol, Transmission control Protocol, User Datagram Protocol, ICMP etc., some of the message Authentication codes, Authentication Header and their IP Security components such as the Encapsulating Security Payload can also be used. Sometimes they also can be blocked on both the sides of the firewalls also.

Firewall Policy based on the Applications

Most early firewall work involved simply blocking unwanted or suspicious traffic at the network boundary. Inbound application firewalls or application proxies take a different approach—they let traffic destined for a particular server into the network, but capture that traffic in a server that processes it like a port-based firewall. The application-based approach provides an additional layer of security for incoming traffic by validating some of the traffic before it reaches the desired server. An application firewall or proxy also prevents the server from having direct access to the outside network. If possible, inbound application firewalls and proxies should be used in front of any server that does not have sufficient security features to protect it from application-specific attacks.

Firewall Policies Based on User Identity

Traditional packet filtering does not see the identities of the users who are communicating in the traffic traversing the firewall, so firewall technologies without more advanced capabilities cannot have policies that allow or deny access based on those identities. One of the most common ways to enforce user identity policy at a firewall is by using a VPN. Both IPSec VPNs and SSL VPNs have many ways to authenticate users, such as with secrets that are provisioned on a user-by-user basis, with multi-factor authentication. NAC has also become a popular method for firewalls to allow or deny users access to particular network resources. In addition, application firewalls and proxies can allow or deny access to users based on the user authentication within the applications themselves. Firewalls that enforce policies based on user identity should be able to reflect these policies in their logs. That is, it is probably not useful to only log the IP address from which a particular user connected if the user was allowed in by a user-specific policy; it is also important to log the user's identity as well.

Firewall Policies Based on Network activity

Firewalls allow the networks to work on the time basis through which all the systems on the networks can gain the benefit. Time-based policies are useful in thwarting attacks caused by a logged-in user walking away from a computer and someone else sitting down and using the established connections. However, these policies can also be bothersome for users who make connections but do not use them frequently. If the user does not save the file back to the file server before the firewall-mandated timeout, the timeout could cause the changes to the file to be lost. A different type of firewall policy based on network activity is one that throttles or redirects traffic if the rate of traffic matching the policy rule is too high. Another policy might be to drop incoming ICMP packets if the rate is too high. Crafting such

policies is quite difficult because throttling and redirecting can cause desired traffic to be lost or have difficult-to diagnose transient failures.

IV. LITERATURE REVIEW

Al-Shaer and H. Hamed. have given firewall detection techniques and policy guidelines The Firewall Policy Advisor significantly simplifies the management of any generic firewall policy written as filtering rules, while minimizing network vulnerability due to firewall rule misconfiguration.

B.Hari, S. Suri and G. Parulkar, defined the packet filter rules and the different techniques of filtering rules. It also defines the classification and security of firewall.

Richard Macfarlane, Prof William Buchanan, Dr Elias Ekonomou, Omair Uthmani, Dr Lu Fan and Owen Lo have proposed the security policies also defines the different types of ;policies based on network system, it also define the low level and high level policies.

Tung Tran, Ehab Al-Shaer, and Raouf Boutaba In their paper they have proposed the tools called policy visualization PolicyVis was shown a very good tool in finding rule anomalies or conflicts easily and quickly

Daniel GHEORGHICĂ1, Victor has defined the firewall and its technologies like packet filtering. They also define the application layer and proxy layers firewalls.

Vadim Zaliva, defines the policy and analysis he proposed the policy model, also defines the anomaly detection techniques. In policy model he defines the rules and in anomaly techniques defines the various anomaly techniques like shadowing, redundancy etc.

Muhammad Abedin, Syeda Nessa, Latifur Khan, and Bhavani Thuraisingham define the representation of rules, relationship between two rules, anomaly algorithm. These rules have to be defined and maintained with utmost care, as any slight mistake in defining the rules may allow unwanted traffic to be able to enter or leave the network, or deny passage to Quite legitimate traffic.

Jitha C K, Sreekesh Namboodiri has given the anomaly detection techniques and policy anomaly discovery. This policy managing tool is practical and helpful for system administrators to enable an assurable network management.

Gail-Joon Ahn, Senior Member, IEEE, and Ketan Kulkarni have proposed a novel anomaly management framework that facilitates systematic detection and resolution of firewall policy anomalies.

W. Eric Wong and Vidroha Debroy has defines the localization methods and software fault localization. , fault localization is the activity of identifying the exact locations of program faults. It is a very expensive and time consuming process

Dr. Alex X. LiuIn assumes that a firewall maps every packet to one of two decisions: accept or discard. Most firewall software supports more than two decisions such as accept and reject. Our firewall design method can be straightforwardly extended to support more than two decisions.

Eppstein and S. Muthukrishnan, highlighted the concept of the Firewall security, like any other technology, requires proper management to provide the proper security service. Thus, just having a firewall on the boundary of a network may not necessarily make the network any secure. One reason of this is the complexity of managing firewall rules and the potential network vulnerability due to rule conflicts.

V. COMPARISON BETWEEN THE FIREWALL POLICIES

List ref	Policies	description	Advantages
1.	**Policy modeling**	Formalize the firewall rules	Define the list of rules for packet filtering
2.	**Anomaly detection**	Detect the anomalies from the sequence of filtering rules	Provide the different methods for detecting firewall anomalies
3.	**Automated correction of policy fault**	Correcting the faults without any side effect other rules	provide the techniques of random packet generations
4.	**Fault localization**	Define the main root and location of the fault	Provide the two approaches for decreases the cost of testing and debugging(RFC and RDC)
5.	**Firewall policy editor**	Helps the user to determine the proper order for a new or modified rule in the policy	provide the method of insertion and removal in the sequence of filtering rules
6.	**Firewall tools**	Help the administrator dealing with complex and time consuming tasks	provide the policy anomaly detector tool.

Table I: Comparison between various firewall policies.

VI. CONCLUSION

From the above study we conclude that proper management to provide the proper security service. One reason for this is the complexity of managing firewall rules and the potential network vulnerability due to rule conflicts. In this paper cover important issues that are related to the firewall policy management. We reviewed recent works on automatic correction and fault localization in two separate sections

REFERENCES

[1] B. Hari, S. Suri and G. Parulkar. *"Detecting and Resolving Packet Filter Conflicts."* In Proceedings of IEEE INFOCOM'00, March 2000.

[2]A. Mayer, A. Wool and E. Ziskind. *"Fang: A Firewall Analysis Engine."* In Proceedings of 2000 IEEE Symposium on Security and Privacy, May 2000

[3]W. Cheswick and S. Belovin. Firewalls and Internet Security. Addison-Wesley, 1995.

[4] S. Cobb. *"ICSA Firewall Policy Guide v2.0."* In NCSA Security White Paper Series, 1997.

[5] Lupu and M. Sloman. "*Conflict Analysis for Management Policies."* In Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM'1997), May 1997.

[6] S. Cobb, *"ICSA Firewall Policy Guide v2.0,"* *NCSA Security White Paper Series*, 1997.

[7]J. Wack, K. Cutler, and J. Pole, *"Guidelines on Firewalls and Firewall Policy,"* *NIST* Recommendations, SP 800-41, Jan. 2002.

[8]A. Wool, *"Architecting the Lumeta Firewall Analyzer," Proc. 10th USENIX Security Symp,* Aug. 2001.

[9]W. Cheswick and S. Belovin, *Firewalls and Internet Security*, Addison-Wesley, 1995

[10]J.A. Jones and M. J. Harrold. *Empirical evaluation of the tarantula automatic fault-. Localization technique*. In proceedings of the 20th IEEE/ACM International Conference on Automated Software Engineering, Pages 273-282, 2005

[11]E. Al-Shaer and H. Hamed. *Firewall Policy Advisor for anomaly discovery and rule editing*. In Integrated Network Management, 2003. IFIP/IEEE Eighth International Symposium on, pages 17–30, 2003.

[12]T. Tran, E.Al-Shaer, and R. Boutaba. PolicyVis: *Firewall Security Policy Visualization and Inspection*. In proceedings of 21st Large Installation System Administration Conference. Nov, 2007.

