Asian Journal of Research in Computer Science

12(3): 25-32, 2021; Article no.AJRCOS.77055
ISSN: 2581-8260

First Line of Defense: Firewall

Yashraj Singh Tomar [a#] and Nayan Bhile [b*#]

[a] Ujjain Engineering College, Ujjain, India.
[b] Shri Vaishnav Institute of Information and Technology, Indore, India.

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2021/v12i330286
Editor(s):
(1) Prof. M.A.Jayaram, Siddaganga institute of Technology, India.
Reviewers:
(1) Seyedeh Yasaman Rashida, Islamic Azad University, Iran.
(2) Sonali Bhutad, Mumbai University, India.
Complete Peer review History: https://www.sdiarticle4.com/review-history/77055

Mini-review Article

Received 02 September 2021
Accepted 12 November 2021
Published 15 November 2021

ABSTRACT

Firewalls are a fundamental element of network security systems with the ability to block network data traffic flows according to predefined rules. They work on the main purpose to prevent the spread of any deleterious event both on the host as well as network side from any intrusion. Conventional firewalls rely on functions specified by a sequence of rules, which often conflict. Also, various forms of tunnels, wireless and dial-up access methods allow individuals to bypass all the security mechanisms provided by the traditional firewall. Thus, in this paper we discuss the uses and classification of both host and network-based firewalls, other firewall approaches to overcome the cons of traditional firewalls, various firewall policies, including some anomalies.

Keywords: Packets; demilitarized zone (DMZ); ports; TCP/UDP; OSI Model; IPSEC; cryptography; firewall decision diagram (FDD).

1. INTRODUCTION

From ancient times when it comes to defending some asset the first idea that strikes someone's mind is to construct a wall, like the Great Wall of China (built by Chinese people roughly 2000 years ago) to defend themselves from the neighboring tribes. Here in this article, we are going to discuss a kind of wall that enforces security policies and becomes the first line of defense for a network.

Student.
**Corresponding author: E-mail: nayanbhile.off@gmail.com;*

A firewall is a guard, interposed at the entry of a network and the extranet, as it resides at the boundary, it is often called "perimeter security" [1]. It monitors the inbound and outbound traffic looking for anomalies and malicious traffic specified by a network administrator. If it finds unauthorized traffic, the firewall blocks the traffic and doesn't allow it to enter the network. This process of either allowing or denying entry into networking is known as packet filtering [1, 2].

With the increase in the use of the internet, the threats are also increasing, due to which, a lot of effort has been put into making the network more secure and robust, and this lead to the development of the firewall. Due to the increase in network attacks, the firewall has become an important part of every network. As stated earlier, firewalls need certain sort of policies or a set of rules to perform filtering. It's really important to define those properly, it could be a problem if those rules have certain anomalies. So special attention must be given to what kind of relation the rules share and the interaction between them.

A good firewall must have the following attributes:

i. All the data flowing to and from the network must pass through the firewall.
ii. The policies must be implemented properly and packets must be allowed as specified in policies rules.
iii. It must keep the track of all the data packets passing through.
iv. It must notify the administrator if a break-in happens.
v. It should be immune to all kinds of attacks.

1.1 Uses of Firewall

One of many use of firewalls is they are used to prevent the spread of any dangerous event i.e. if in any case firewall fails to prevent intrusion and one of the "demilitarized zone or DMZ" gets compromised, then it can stop the propagation of malware as no traffic can bypass the firewall [1]. Another use of a firewall is to prevent access to critical information by blocking certain classes of web content from certain categories of hosts (e.g. libraries, schools, colleges, etc.). It also prevents the unnoticed and unauthorized leak of data. Last but not least, firewalls could be used for auditing in the situation of a breach, also monitoring employees' actions over the network.

So, here in this article, we will discuss the classification, advantages, and threats against the firewall along with firewall policies.

2. CLASSIFICATION OF FIREWALL

Firewalls are broadly classified into two parts based on the location where the firewall is placed. They are:

2.1 Host-based Firewall

This kind of firewall is software that comes as a part of the operating system. They are placed on the nodes of a network. It prevents attacks at a specific host location [3].

2.2 Network-based Firewall

This kind of firewall works at the network level and is located right of the entrance, from here it inspects data traffic and filters it [3].

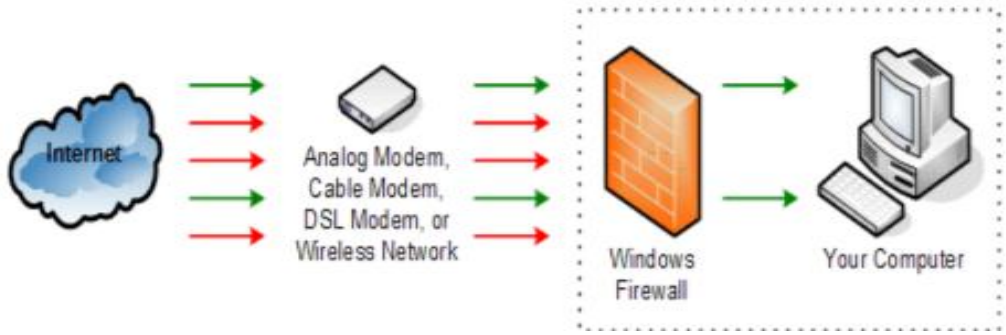

Fig. 1. General working of a firewall [3]

These firewalls can be further divided into:

i. Packet Filtering Firewall
ii. Circuit Filtering Firewall
iii. Application Gateway Firewall

2.3 Packet Filtering Firewall

The main functionality of a packet filtering firewall is to look at the headers of packets traveling through it, checking information like Source IP address, destination IP address, transport-level protocol, TCP/UDP source port or equivalent and TCP/UDP destination port or equivalent, and the packet direction of propagation (i.e. inbound or outbound). After analyzing the packet header and comparing it with the policies it either allows or blocks the packet [1].
Some of the advantages of Packet filtering firewall:

i. Their functionality is quite simple and hence is fast and efficient.
ii. They can work independently i.e. they don't require any kind of cooperation by a user.
iii. These are cost-effective (are very cheap).

Some of the drawbacks of Packet Filtering Firewall:

i. The first and most important drawback is it's really hard to write the correct filter.
ii. It can't identify the user causing the traffic although it can identify the IP, but to keep the track of a host is a challenging task (a user can spoof his/her IP address).
iii. Local machines can spoof other local machines

Despite this, another problem is that a remote host could send a different packet (which is not part of an established connection) which could pass the packet filter not keeping the track of a TCP session. To avoid this we can keep the track of the state of a TCP connection and such firewalls are called the Stateful packet filters firewall, Adaptive firewall, or Packet inspection [1]. Such kind of filters keep keeps their eyes on both network level as well as transport level data.

2.4 Circuit Filtering Firewall

A circuit-level firewall works at the session layer of the OSI model. As it works at the session layer, it is simple to predict what it is supposed to do, it monitors the handshake of the packet and decides if it is legitimate or not. In simple words, a virtual circuit exists between the host inside the protected network and the proxy server, as any inner host sends a request to the external host, it is interrupted by the circuit proxy and it changes the original IP address with its IP address and then forwards it to an external host. As a response comes, instead of going to the host inside, it goes to the proxy server. It checks the IP and Port if they are safe and trusted and allows the response to pass by and send it to the dinner host.

So this gives us a major advantage that any non-requested data can't enter the network. Another big advantage is that- external host can't see the internal system as all the communication is being held between the proxy server and the external host.

Despite this, a disadvantage is that if we don't use any other filter, then all data requested out of the network would be allowed to pass.

2.5 Application Gateway Firewall

This proxy at the application level is better than transport-level proxies. They can enforce application-level protocol and prevents abuses of the protocol by both client and server. This is better than a circuit-level firewall because it not only checks the source and destination IP address, source and destination port, TCP header information, but also the content of the packet [4]. It can judge whether the data is a threat to the network based on the amount of information available.

2.5.1 Some advantages of Filter here is based on actual data:

i. Filter here is based on actual data.
ii. Ensures the proper implementation of protocols.
iii. Can limit the user's communication based on the authorization.

2.5.2 Some disadvantages of Application Gateway Firewall:

i. These are slow in context to speed of data flow (due to proxies' application).
ii. The application-level firewall needs to be configured at the client device.

iii. They are on the expensive side compared to other firewalls.
iv. Doesn't work for many protocols and different protocols need different proxies

A firewall can be divided into 2 types based on whether it keeps the track of packets or not.

i. **Stateless firewall:** This kind of firewall decides the fate of a packet based on the packet itself, no other information is taken under consideration [5].
ii. **Stateful firewall:** This kind of firewall decides the fate of a packet based on the packet itself, along with the information of previously accepted packets. (It keep the track of information of what kind of packets are passing through it) [5].

3. OTHER APPROACHES

Other than the above-discussed firewalls, some other approaches can be used to implement a firewall.

3.1 Distributed Firewall

Conventional firewalls depend on the topology of the network to enforce the traffic filtering, but the problem here is an assumption that all the hosts inside the protected network are trustworthy. Still, it worked well for the small and medium-sized network, but due to increased use of network, high-speed requirement, its conventional firewalls are not able to cope with all these changes.

To resolve this problem Steven M. Bellovin came up with the idea in [6]. He showed that policies are still centrally defined, but the implementation of this policy is enforced at the endpoint. In case if attacker penetrates the outer defenses (other firewalls) then the individual device inside the protected network is responsible for its part of the security policy, which makes each device more secure, and instead of getting inside the network attacker won't find any vulnerable target.

The Implementation of a distributed firewall depends on three components, which are:

i. A good language to define the policies which specify which connection is permitted and which is blocked.
ii. A proper safe policy distribution system.
iii. Mechanism to enforce the security policy on the traffic.

Here comes the next problem, how to identify the host. The most common host designator is IP. However, spoofing IP is easy and reduces the level of security. Instead of using an IP, we use the name of a cryptographic certificate used with IPSEC. It's a reliable and unique identifier. It can't be spoofed easily. Also with this kind of firewall no DMZ or screened network is no longer needed [6].

3.2 Structured Firewall

In a conventional firewall, the policy was defined as a list or sequence of rules which cause some problems. Such as the consistency problem, completeness problem the compactness problem. In order to resolve these problems, the concept of structured firewall design was proposed.

It can be said that its implementation comprises of two steps-

i. The first step involves designing a firewall using a firewall decision diagram (FDD).
ii. The second step involves the conversion of this diagram into a sequence of rules using a program.

These 2 steps resolve all the above-discussed problems. An FDD is free of conflict within the rules and its syntactic requirement makes it mandatory for the designer to consider all kinds of traffic which resolve the first 2 problems (consistency and compactness problem). In the second step, we use 2 algorithms to make rules out of FDD- one is known as FDD reduction and the other is known as FDD marking. Other than these 2 algorithms, we use an algorithm to remove redundancy from the rules which mitigate the third problem of compactness [5].

Any sort of change in firewall policy can cause a huge hole in the firewall, which could eventually cause a big problem. But if we use a structured firewall then the administrator only needs to modify the firewall decision diagram. After which he/she could use the programs to automatically generate the sequence of rules.

4. FIREWALL POLICY

As we all know from previous discussions firewall is the first line of defense for a network, and its proper deployment is a top priority. Firewall policy decides the effectiveness of firewall security.

Referencing from [7], it can be said that a firewall policy is a set of rules which is used by a firewall to:

i. Determine what traffic your firewall allows and what is blocked.
ii. Examine the control information in individual packets, and either block or allow them according to the criteria that you define.
iii. Control how the firewalls protect your network from malicious programs and unauthorized access.

In their paper, Smriti Salaria and Nishi Madaan gave a descriptive analysis of various firewall policies. Let us look into each of them by first looking at the following comparison chart-

4.1 Firewall Policy Modeling

In order to develop a firewall successfully, one of the very first steps includes modeling the firewall policies. It requires several high-level languages (even sometimes graphical) in order to define a firewall policy. Well, in this case, the representation of the firewalls is required to be translated into the native policy descriptive language of an actual firewall platform. Some examples are- Firewall Builder [9], HLFL, FLIP [10], Firmato [11], INSPECT, XACML [12].
These languages can be used to define a policy of a firewall or to define an organization's policy files for multiple firewalls. Vadim Zaliva has mentioned and illustrated some modern examples and implementations of such models in his paper [13].

4.2 Anomalies

To deploy a firewall properly we need to define a firewall policy without any anomaly, which needs a considerable amount of care, experience. Managing a firewall, especially for an enterprise network is complex and error-prone. So we can say that while we are dealing with thousands of these rules, having conflicting or redundant rules is an easily possible case.

Keeping that in mind, H. Hamed and E. Al-Shaer discussed some anomalies in [14] which are as follows-

i. **Shadowing anomaly:**

A rule R1 shadows rule R2 if all the packet matches the rule R1 in which case no rule R2 is of no use and it won't be activated ever. Due to this kind of anomaly, the traffic intended to be allowed can be denied and traffic to be denied could be allowed.

ii. **Correlation anomaly:**

Two rules are in correlation if they can match each other's packet but their filtering actions are different. This is considered an anomaly because they combined imply the outcome that was not explicitly stated in the rules. For example- if two rules deny some traffic from a sender to a receiver. If their order is reversed then it would allow the same traffic to pass through.

Table 1. Comparison between various firewall policies [8]

Sr. No.	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 effects 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 decreasing 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 deal with complex and time-consuming tasks	Provide the policy anomaly detector tool.

iii. **Generalization anomaly:**

A rule is the generalization of the preceding rule if they have a different action, but the first one can match all the packets that match the second rule. Generalization is generally used to exclude certain traffic from a general rule. This is considered an anomaly because if not placed properly then traffic to be blocked could be allowed, and allowed traffic may get blocked.

iv. **Redundancy anomaly:**

A rule can be said to be redundant if it matches all the packets that another rule matches and have the same filtering action can be said redundant rule. It's an error because it adds to the size of rules and increases search time.

v. Irrelevance anomaly:

A rule is said to be irrelevant if it doesn't match any traffic that may flow through the firewall. This is considered an anomaly because it adds unnecessary overhead to the filtering process and does not even contribute to the policy semantics.

4.3 Automated Correction of Policy Fault

Though we place firewalls between our private network and the outside internet so that all the incoming packets can be filtered and discarded when required, but most of the firewalls contain faults and poor configuration which then results in the allowance of unwanted/ malicious traffic unnecessarily. In order to overcome this, firewalls that can automatically correct the faults are introduced.

Some of the very often faults that are found in the firewalls include wrong order, missing rules, wrong decisions, wrong predicates, and wrong extra rules. All these faults were detected and countered separately and automatically in the comprehensive fault model in [15]. Despite this, there are also many security policy companies such as 'Tuffin' who progress daily to encounter such problems. For example- Karen Crowley, in her blog [16] clearly mentioned the automation approach of their company towards automated correction of their faults.

4.4 Firewall Fault Localization

Faults that happen to be there in any firewall need to be fixed, for that, finding the fault is more important, and even more important is to find the root of that fault. Finding the root of the fault is known as fault Localization.

There are two approaches to decrease the cost of debugging and fault localization [8]. They are-

i. **RDC (Rule Decision Change)** - If faults are found in this category, it shows that the rule's decision is incorrect.
ii. **RFC (Rule Field interval Change)** - If faults are found in this category, it shows that the field interval in the rule is incorrect.

Faults found under these categories indicate that there is one or more fault in the rule or the structural entity (e.g. decision). Any false rule in the structural entity is a critical one to be corrected and needs to be mitigated as soon as possible.

4.5 Firewall Policy Editor

Editing policies are as much as important as creating them. With the time-passing, new rules and policies are required to be added to the firewalls to enhance and update the security as per the requirements and changes in the network topology. With the help of a policy editor, this task can be done with ease. The policy editors are designed in such a way that it makes it easier for the user to edit a rule in any context as sometimes, it also provides an overview of both the rules and the entire policies.

4.6 Firewall Tools

Daily advancements in networking techniques and security policies require regular updating of firewalls with them. Misconfigurations, unused rules, or conflicting rules can be reasons for a firewall to fail in doing its purpose. Hence, in order to successfully accomplish this task, several firewall tools are designed to manage the firewall policies in an easy way for the user. Examples of such tools are- Tufin, AlgoSec, FireMon, and RedSeal [17].

Order	Protocol	SrcIP	SrcPort	DestIP	DestPort	Action
1	tcp	140.192.37.2	*	161.120.33.*	20	ACCEPT
2	tcp	140.192.37.*	*	161.120.33.42	20	DENY
3	tcp	140.192.37.*	*	161.120.33.41	25	ACCEPT
4	tcp	140.192.37.1	*	161.120.33.41	25	DENY
5	tcp	140.192.37.3	*	161.120.33.43	21	ACCEPT
6	tcp	140.192.37.*	*	161.120.33.43	21	DENY
7	tcp	140.192.37.*	*	161.120.33.44	53	ACCEPT
8	tcp	140.192.37.4	*	161.120.33.44	53	ACCEPT
9	tcp	140.192.37.5	*	161.120.33.44	23	ACCEPT
10	tcp	140.192.37.5	*	161.120.33.44	23	DENY
11	tcp	140.192.37.5	34	161.120.33.45	22	ACCEPT
12	tcp	140.192.37.*	35	161.120.33.45	22	DENY
13	tcp	140.192.37.1	*	161.120.33.42	20	DENY
14	udp	*.*.*.*	30	161.120.33.43	50	ACCEPT
15	udp	140.192.37.*	30	161.120.33.43	50	DENY

Fig. 2 (Packet filtering rules)

5. FILTERING RULE FORMAT

Any field in a TCP, UDP, or IP header can be used in the filtering rule. But most commonly used fields are protocol type, source IP address, destination IP address, source port, destination port. Packets are permitted or blocked based on the rules whose all field matches the header information. If the rule doesn't match, then we jump to the next rule until a matching rule is found or a default policy is reached. One more thing is the order of arrangement, firewall rules are order sensitive. Fig .2 shows an example of a packet filtering rule.

The table above contains 15 rules. Let's discuss a rule to have a better understanding. Talking about rule-1, it says if the protocol is TCP and the packet is coming from 140.192.37.2 from any port number (* covers every possible value) for the destination 161.120.33.* (it means every destination with initial address 161.120.33.) and port 20 must be allowed to enter the network.

Now, let's look into rule-14 and rule-15. If a UDP packet arrives from any source IP and port-30 to the destination IP- 161.120.33.43 at port-50, then the packet will be allowed (as per rule-14). But, an exception is stated in rule-15 i.e. if any UDP packet arrives from source IP- 140.192.37.* and port-30 to the destination IP- 161.120.33.43 at port-50, then, in this case, the packet will be blocked.

6. CONCLUSION

In this paper, we discussed the fundamental functions and brief introduction of firewalls also what are their uses and what attributes that a good firewall must possess are. We have discussed the classifications of the firewall as host-based and network-based firewalls. Firewall security, like any other technology, requires proper management to provide the proper security service. Thus, just having a traditional firewall on the boundary of the network may not necessarily make the network secure. So, we discussed some other firewall approaches such as distributed firewall and a structured firewall. The proper deployment of a firewall is a top priority, hence we have discussed some firewall policies for the effectiveness of firewall security. At last, we ended our discussion on firewalls by a discussion on some anomalies which may occur to a firewall.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Network Firewall. Kenneth Ingham, Stephanie Forrest. January, Research Gate, 1994;52.
2. Simple and Flexible Datagram Access Controls for Unix-based Gateways. Mogul, Jeffrey C. Palo Alto, California : s.n., March, Western Research Laboratory; 1989.
3. Secure Collecting, Optimizing, and Deploying of Firewall Rules in Software-Defined Networks . Sunghwan Kim, Seunghyun Yoon, Jargalsaikhan Narantuya, Hyuk Lim. December, IEEE Access. 2019;5.
4. Thinking about Firewalls. Ranum, Marcus J, ELSEVIER, 1997;8.

5. Structured firewall design. Mohamed G. Gouda, Alex X. Liu. September, ELSEVIER, 2005;9.
6. Distributed Firewalls. Bellovin, Steven M.. November, smb@research.att.com, 1999;11.
7. Diverse Firewall Design. Alex X. Liu, Mohamed G. Gouda. September, IEEE Computer Society, 2008;3.
8. Firewall and Its Policies Management. Er. Smriti Salaria, Er. Nishi Madaan. April, International Journal of Computer Science and Mobile Computing, 2014;9.
9. Platform-Independent Firewall Policy Representation. Zaliva, Vadim. December 2007;22.
10. Specifications of a high-level conflict-free firewall policy language for multi-domain networks. Bin Zhang, Ehab Al-Shaer, Radha Jagadeesan, James Riely, Corin Pitcher. 2007:185-194.
11. Firmato: A novel firewall management toolkit. Y. Bartal, A. Mayer, K. Nissim, A. Wool. August 06, , IEEE Xplore, 2002; 40.
12. Simon Godik, Tim Moses. eXtensible Access Control Markup Language (XACML). s.l. : OASIS Standard; 2003.
13. Firewall Policy Modeling, Analysis and Simulation: A Survey. Zaliva, Vadim. May 9, 2008:11.
14. Modeling and Management of Firewall Policies. Ehab S. Al-Shaer, Hazem H. Hamed. Apri, Institute of Electrical and Electronics Engineers (IEEE), 2004;10.
15. First Step Towards Automatic Correction of Firewall Policy Faults. Fei Chen, Alex X. Liu, JeeHyun Hwang, Tao Xie. s.l. : ACM Digital Library, July 30, ACM Transactions on Autonomous and Adaptive Systems; 2012.
16. Crowley, Karen. https://www.tuffin.com. [Online] September 14, 2017. Avaialble:https://www.tufin.com/blog/3-ways-get-started-firewall-automation.
17. 4 tools for managing firewall rules. s.l. : CSO; 2016.
18. Implementing a Distributed Firewall. Sotiris Loannidis, Angelos D. Keromytis, Steve M. Bellovin, Jonathan M. Smith. April, ResearchGate, 2001;9.
19. Research on Computer Network Security Based on Firewall Technology. He, Xinzhou. November, Journal of Physics: Conference Series. 2009;6.
20. Overview of Firewalls: Types and Policies. Salah-ddine Krit, Elbachir Haimound. Managing Windows Embedded Firewall Programmatically, 2017;7.
21. Case Studies of SCADA Firewall Configurations and the Implications for Best Practices. Dinesha Ranathunga, Matthew Roughan, Hung Nguyen, Phil Kernick, Nickolas Falkner. December, IEEE Transactions on Network and Service Management, 2016;14.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle4.com/review-history/77055