International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Rules Assurance: Preventing Unauthorized Access through Building Right Firewall Configuration

K. Shyamala, G. Priyadharshini

Abstract: ***Any business organization's backbone is their infrastructure which establishes the connection between their own intranet, vendor/customer network and external world. Network is linked between these network are through dedicated connection or public connection via internet. To build any network, it requires servers, firewalls, routers, core and access switches with communication link. The topology of network, link type, usage of network devices are chosen based on organization need and type of data transaction flows between these networks. Considering volume of data growth because of digital revolution, sensitiveness of data like Personally Identifiable Information (PII) or Protected Health information (PHI), it is necessary to protect data from hackers and save network from phishing, malware or ransomeware. Firewall will control the access and decides what to allow or deny between networks. These rules are defined in firewall Access Control List (ACL). A strong, well matured access control policy plays a key role to ensure network security and data protection. A firewall rule defines inbound and outbound data traffic between source and destination. These sources and destinations are identified by IP addresses, subnet ranges, protocols, applications, and port numbers. ACL defines what can be accessed / denied from internal (OUT BOUND) or from external (IN BOUND). In general a firewall has hundreds of ACLs and at times in thousands as well. Since frequent changes are inevitable, managing firewall rules becomes a complex task. There is no relationship between these rules and need not be in an order. Firewall will not validate duplicate or overlapping of rules. Every rule in ACL is independent and there are more possibilities of having obsolete and invalid rules. To overcome all these complexities, this wok presents rules mining, which helps to analyze firewall rules, identify security flaws, vulnerabilities from existing rules and eliminate redundant or unused rules from network. This paper proposes a new guidelines that can be used on existing firewall ACL or while building new firewall ACL to protect network from external sources. These guidelines will help network administrators to fix configuration errors.***

Keywords : Network security, data protection, firewall, ACL, network rules, running configuration, Data protection, Data privacy..

Manuscript published on 30 September 2019
* Correspondence Author
Dr.K.Shyamala*, Associate Professor Department of Computer Science , Dr. Ambedkar Government Arts College, Chennai, India.
G.Priyadharshini, Research Scholar Department Of Computer Science , Dr. Ambedkar Government Arts College, Chennai, India.

I. INTRODUCTION

Firewall is a network security system that prevents unauthorized access of incoming and outgoing network traffic by enforcing security policies. Firewall acts as a filter between the network and the computers in any business organizations or institutions. Each and every packet that flows through the network is monitored and filtered. Using firewall, a barrier is established between the trusted internal network (Computers in an organization) and untrusted external network (Internet). Firewall scrutinizes all incoming and outgoing data packets and decides which packets should flow through the network.

Firewall can be set up which reflects the security policies of an organization. Firewall can be implemented by a set of code that enforces the security policies. Figure 1 shows the basic firewall setup. Firewalls block traffic intended to specific IP addresses or server ports.

A Trusted network is a network which comes under the control of network manager or administrator that allows authorized users to transfer data in a secured manner. The trusted networks should have the features like authentication, encryption, firewall and a private network.

DMZ or demilitarized Zone acts as an isolated network placed between the internet and internal network. The primary function of DMZ is to prevent public services provided to the external network from the resources in the internal network. To create a demilitarized Zone, two firewalls will be deployed. One firewall is connected to the internet and another firewall is connected to the internal network. In between these two, DMZ will be deployed

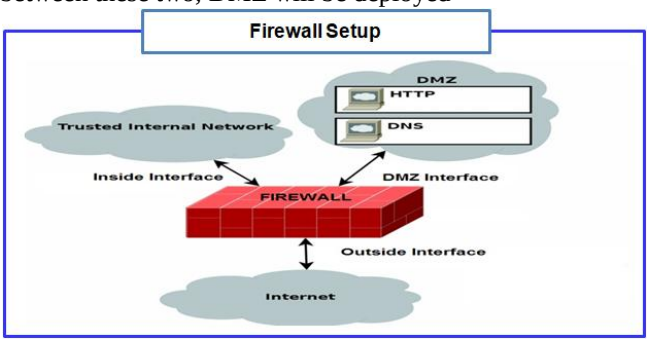

Figure 1 Typical Firewall Setup

A. Firewall Interface

The main function of the firewall interface is to decide what traffic can be allowed to traverse from one direction to the other. Figure (2) shows the three types of interfaces used in the firewall setup.

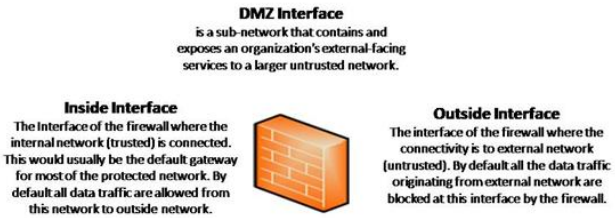

Figure 2 Types of Firewall Interface

External interface: This interface is connected to the external network (untrusted network). All the packets originating from external network are filtered at this interface.
Internal interface: This interface is connected to the internal network (trusted network). This would be the gateway for the protected network. All data traffic from this network is allowed to outside network.
DMZ interface: It is a sub-network that contains and exposes an organization's external facing services to a large untrusted network

B. Firewall Types

Table (1) shows the different types of firewalls, protection level, strength and weaknesses.

S.NO	FIREWALL NAME	PURPOSE	PROTECTION LEVEL
1	Traditional network firewall	Provides network protection by preventing unwanted traffic in to corporate network	high
2	Next-Generation firewalls(NGFWs)	Provides network protection by looking at the contents of data packet rather than its port, source and destination IP address	Very high
3	Web Application Firewalls	This is usually a proxy server analyzes the data to filter malicious request	high
4	Database Firewalls	Specifically designed to detect and prevent database attacks	high
5	Unified Threat Management (UTM) appliances	Includes features like traditional firewall, intrusion detection and internet gateway security	Medium
6	Cloud Based firewalls	An alternative to firewalls running from the corporate data centre and protects networks, applications and databases	high
7	Container firewalls	A container firewall is used to protect and isolate containerized application stacks, workloads and services on a container host	Medium

II. Problem Statement

All security threats occurred because of incorrect configuration of firewall ACL. Breaches will not happen because of faulty software if it is well protected by firewall. As per Gartner's recent survey [3] more than 95% of breaches are occurred because of firewall misconfiguration. Incorrect of firewall rules not only impacting the performance of network, but also laid path for potential attack by external. When rules are incorrectly configured, outside resources which shouldn't have access to the network, will get access and destroy the entire system and steal sensitive data. Hence it is important to have error free firewall configuration. When breach occurs through firewall, it is not only impacting the business, but also resources like people, server, and other network. Since there are no proper tools available to validate or troubleshoot ACL, most of firewalls have errors which are not easily identifiable by normal user. Error in firewall rules will open path to allow malicious traffic into private network or restrict legitimate traffic. When malicious traffic is allowed, they can attack network easily. At the same time, when restricting legitimate traffic, it will have huge impact on business aspect.

Changes on ACL are frequent and are managed by various firewall administrators at different times for multiple business cases. A firewall can have huge number of rules, sometimes in thousands which are logically entangled and there is no order of preferences for these rules. There is also more possibility of conflicts between these rules like the same IP address or range of IP addresses occur in both permit and deny rules. With capacity of human capabilities, it is not easy to validate and troubleshoot huge list of rule and complex scenarios.

SANS technology institute's research [1] reveals the reason for top firewall leaks. They mentioned that common flaw in most firewall ACL is that network allows everything towards the internet and allows all ports. Some of traffic patterns which lead to network breach are listed below

- Since there is minimal or no controls are placed on outbound access, encrypted channels like SSH, SSL are not scrutinized as the data stream is already encrypted
- Using third party VPN solution for connecting between corporate network
- Allowing outbound VPN sessions to perimeter

A. Research Objective

To build trusted and stable network, it is important to build right set of firewall which permits only verified INBOUND and OUTBOUND connections. This research mainly focusing on how to verify firewall rules to ensure all rules are valid. These steps will help firewall administrator to eliminate obsolete rules, identify duplicates and remove them on regular intervals. This will also focusing on how to avoid overlapping of access when we use subnet ranges. For example, one rule may allow set of IP ranges to access network and subset of this IP range will not be allowed to access our network in another rule which may not execute at all.

As per recent study on" Strategy and Solution to comply with GDPR" [7], it is important to restrict unauthorized access to network perimeter to prevent data leakage. This can be accomplished through defining proper firewall rule and make sure only authorized personnel are having required access for specific duration. Access control list must be reviewed on periodic basis, at least once in 3 months. This research work helps firewall admin also focusing on explain how to sequence all rules while configuring firewall

III. Literature Review

Since there is a lack of tools for verification and troubleshooting of firewall policies, Alex X.Liu [2] proposes tool for firewall verification and troubleshooting. The firewall policy and a given property is taken as input and the output specifies whether the policy satisfies the property.

This tool also identifies the rules causing verification failure. A verification and troubleshooting algorithm has been designed and implemented using decision diagrams.

Ahmed Khoumsi, Mohammed Erradi, Wadie Krombi et al [4] presents a firewall security policies which is based on automata method. A method is proposed to identify the white list and black list of firewall rules.

Firewall misconfigurations is a very common problem in network operations. Identifying and removing misconfigurations has become a vital problem to be solved. Amina Saadaoui, Nihel BenSouayeh, Adel Bouhoula et al. [5] addresses this problem by data structure (Firewall Decision Diagram FDD). A procedure has been presented to optimize, clean up and remove superfluous rules and to detect and fix misconfiguration.

G.Wang et al.[8] proposesan approach that checks the conflicts between firewall rules and firewall policiesbasedon the entire flow paths within an open flow network

IV. PROPOSED SOLUTION

When firewall rules and running configuration is not correct, it leads to security threat to the organization. To avoid any firewall breach, it must be configured without any errors as well as close all vulnerabilities through set of guideline to ensure the network is protected from external and reduce overhead of firewall management

A. Nomenclature standardization of Object names

Typically firewall rules are not configured by single person and multiple people will be involved because the rules are maintained for longer duration. In general, team are not using common naming convention while defining object group. The group can be defined by its domain name system (DNS) or IP address or by some name

Figure 3 Service details used in Firewall rules

For example, the above database server can be referred in various ways in firewall rules. Some of them are listed in table 2

Table 1 Various types of services used in Firewall

Method	Example
By IP address	access-list permit any host 10.3.5.1 host 172.2.9.19
By DNS name	access-list permit any host db.dagac.com host 172.2.9.10
By Generic Name	access-list permit any host szone-db-10.3.5.1 host 172.20.59.11

When a firewall has hundreds or even thousands of rules, identifying purpose of added source will not be known and there is a possibility of duplicating same IP address. Also when IP address of a server changes, instead of updating specific rule, security personnel will add additional rule with new IP address and keep old rule as well. In such scenarios, firewall rules will end up having obsolete rules

B. Grouping of similar objects

For easy maintenance, it is always good to group IP addresses or DNS as per usage and category. This is really useful when access rules are built for internal usage like primary, secondary and backup devices. By grouping similar object prevent unused rogue services from network

Without Object group	With Object group
Access-list 100 deny host www.youtube.com Access-list 100 deny host www.facebook.com Access-list 100 deny host www.instragram.com Access-list 100 deny host www.twitter.com	object-group network SOCIAL-MEDIA-URL network-object host www.youtube.com network-object host www.facebook.com network-object host www.instragram.com network-object host www.twitter.com access-list 100 deny ip object-group SOCIAL-MEDIA-URL any4

C. Selection of Firewall Models

In an organization, when we are having different zones which are interconnected, all can share single firewall if usage policy is same and there is no sensitive transaction between zones. This is represented in first sequence of the figure (4).

If zones are dealing with sensitive information and its access need to be managed individually, then all zones are connected to firewall via dedicated port as mentioned in second sequence of figure(4)

When we have to manage large number of zones, it is difficult or not possible to allocate port for each zone. So, dedicated firewall to be installed for each zone which in turn connects with firewall as explained third sequence of figure (4). The disadvantage of this model is that it requires more data center space and maintenance cost. As per recent study [6] increased data center space leads to increased power and operational cost. So, to avoid managing multiple firewalls, virtual firewall can be installed to deploy more firewalls in network

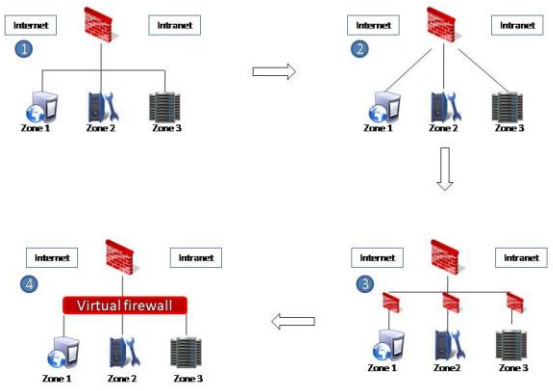

Figure 4 Rule Design for Zones, Service and Network

D. Cleanup rules

- Validate all shadowed rules. Reduce shadowing as much as possible. The shadowed rules must be analyzed and sorted based on the services and remove rules that are effectively useless
- Delete obsolete and unused rules. These rules can be chosen based on hit count of all IP addresses
- Order the rules based on hit count. Rules which are having maximum hit should come first in order.

- Don't keep any connections which are not in use. It covers all source, destination and service routes
- Revisit all policies on regular intervals and delete which are not required.
- Remove redundant objects, for example, some devices may be defined more than once with multiple names
- All rules must be documented with details covering object details, rules, policies, usage and for easy reference

E. Prepare rules matrix to avoid "Go anywhere with any service policy configuration"

Firewall configurations can be done either as white listing policy or block listing policy. White listing policy deny all inbound traffic and accepts rules which are explicitly written to permit access. Block listing policy is compliment of white listing. This policy allows all inbound traffic to network and deny rules which are written in running configuration.

In general, firewall rules are configured in combination of white listing and block listing policy. Since IT team may not have guideline on what to permit and deny in network. So, rules are written with an open policy of allowing any traffic to any service. So, the network is fully exposed to external world.

To avoid such flaws, all applicable rules must be documented with source, destination, services, application and action. As a best practice, firewall admin regularly review the rules with relevant stake holders which makes sure the policy has all new applications and old ones are removed from policy. A sample matrix is shown in table 4

Source	Destn	Services	Action	Log	Status
10.3.5.1	172.2.9.19	http	Permit	No	Active
ROUTER-G	SYSLOG-G	tcp	Permit	Yes	Active
Any	BLOCK-IP	ip	Deny	No	Active
Domain-G	NTP-G	ip	permit	No	Active

F. Last rule will be deny ALL

A well protected network's firewall will have last rule as any/any/ Deny. This stage can be achieved only when we have all rules defined in order. This can be achieved by following steps

Permit ALL rules with enabling log

When administrator don't know about sources, required services allow all rules by enabling log

Table 2 Step(1) Permit ALL with log

Source	Destination	Services	Action	Log	Status
Any	Any	Any	Permit	Yes	active

Permit known rules

By analyzing log, identify trusted connections and add include them either individual sources or subnet range . Ensure all trusted connections are covered in Firewall rule. Once all rules are included, last any/any/deny rule will collect very less or zero logs

Table 3 Step(2) Permit known transactions

Source	Destination	Services	Action	Log	Status
10.0.0.0/24	192.168.0.1	HTTP	Permit	No	active
10.7.3.2.1	192.168.0.1	HTTP	Permit	No	active
Any	Any	Any	Permit	Yes	active

Change last rule as any/any/deny

Once all rules are captured and covered in policy, the control will not go to last line. In this stage, change action from permit to deny and remove log so that the network will be protected well.

Table 4 Step(3) Deny ALL and remove log

Source	Destination	Services	Action	Log	Status
10.0.0.0/24	192.168.0.1	HTTP	Allow	No	active
10.7.3.2.1	192.168.0.1	HTTP	Allow	No	active
Any	Any	Any	**Deny**	**No**	active

V. DESIGN APPROACH

A. Examine Firewall rules

To setup trusted network, a firewall will have set of rules. The individual rules are called firewall rules, From this full set of firewall rules, a rule which actually interacts at that point of time is called firewall running configuration. The Syntax of firewall rule command line is given below for explanation purpose. This syntax is applicable only for CISCO

Access-list <ACLName> <Rule Action>> <Protocol> <Source> <Destination> <port>

To validate firewall, one should know the following before review

- Interface connection details
- Source and destination details with IP address or subnet ranges
- Port open detail for all rules
- Protocol type (TCP/UDP)
- Type of action (Permit / Deny)

B. Validate Firewall rules

Before building firewall, one must know complete detail about network and firewall. Any rule which is defined in firewall must have valid business reason with correct host, service port and validity of rules. Some rules may be created on temporary basis which has to be removed on time. Order of rules must be reviewed as rules are executed from top to bottom. If an IP address is permitted in the beginning and then same IP address is denied, running configuration will never execute deny rule as it is already permitted.

C. Compliant with Security Policies

Firewall rules must comply with all security policies associated with organization, customer and other local regulations.

For example, when a country imposed restriction on pornography, or an organization's restriction on public email or social networking, firewall rules ensure that all such external parameters are covered and adhere to security compliance

D. Monitoring of rules usage

Firewall rules usage report and log are monitored on regular intervals. This helps to identify the rules which are obsolete and not in use. Heavy hit rules which are valid are to be positioned at the top whereas less hit rules will be positioned at the bottom of firewall rules database

E. Follow Change Management Process

Any changes on firewall rules must undergo proper change management process of organization. It must be reviewed by external resource who is independent of network and Subject Matter Expert (SME) in network security

F. Checklist for firewall review

The following are the check lists to be made during the review of firewall.

- Identify the different firewall interfaces
- Look for interfaces that are configured but not in use
- Rules should be analyzed, based on the traffic flow
- Check if the standard banner has been configured as per organization policy
- Check for users who have access to firewall
- Check how the administrators connect to the firewall (ssh or telnet or management console?)
- Check for access to the firewall and if a stealth rule has been configured
- Check for rules which have 'ANY' in source, destination or ports and ensure the specific IPs/Ports are granted access
- Check for rules which are bi-directional (Does the traffic really need it?)
- Check for rules which are denied later, but allowed in a rule above
- Check for rules where access is allowed more than necessary (eg. Access given to a network range where only two hosts need it)
- Check for rules which have been defined for temporary purposes and left as it is Check for rules which are obsolete

VI. Conclusion And Future Work

It is important to ensure our network is safe from malware, ransomeware and other sources. Firewall ACL plays vital role for network security This paper provides a procedure to build and review any firewall rules which helps to identify weak rules and remove them from the list. It also explains order of sequence rules to improve performance of network and reduce cycle time to validate rule. Most of time, overlapping of subnet range, or improper usage of source and destination paves way to hackers to access network. This work addresses this issue and guidelines to prevent them.

This paper also provides checklist which can be used while configuring new firewall or reviewing existing firewall. As a general practice, any rule change will undergo change management process as per industry standards. These guidelines helps change management team to validate the change request. As a next step, few sample firewall rules will be examined by implementing these guidelines to measure efficiency.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors

REFERENCES

1. https://www.sans.edu/cyber-research/security-laboratory/article/top-firewall-leaks
2. Huth, C.L., Chadwick, D.W., Claycomb, W.R. et al. – Information system Frontiers- springer US-arch 2013, Volume 15, Issue 1, pp 1–4
3. http://www.gartner.com/DisplayDocument?id=2254717&ref=g_sitelink
4. Ahmed Khoumsi, Mohammed Erradi, WadieKrombi et al. Journal of King SaudUniversity- computer andInformation Sciences (2018) 30,51-60
5. Amina Saadaoui, Nihel BenSouayeh, Adel Bouhoula et al. Journal of Computational Science 23(2017)181-191.
6. Dr A. Murugan, AND T. Suresh, "Cold LOGIK and RDHX Solution for Data Center Energy Optimization" International Journal of Engineering & Technology [Online], Volume 7 Number 3.4 (25 June 2018)
7. G. Priyadharshini and Dr. K. Shyamala, "Strategy and Solution to comply with GDPR : Guideline to comply major articles and save penalty from non-compliance," , pp. 190-195. doi: 10.1109/I-SMAC.2018.8653696 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8653696&isnumber=8653599
8. G.Wang et al."Towards a security enhanced Firewall Application for open flow Networks"CSS 2013,LNCS 8300,@ SpringerInternationalPublishing Switzerland 2013.
9. https://www.lifewire.com/how-to-test-your-firewall
10. Alex X.Liu "firewall policy verification and Troubleshooting" Computer Networks 53 (2009)2800-2809 ELSEVIER

AUTHORS PROFILE

Dr.K.Shyamala is working as Associate professor in PG & Research department of computer science , Dr. Ambedkar Government Arts college, Chennai, India. She has completed her masters degree in computer science, M.Phil and Ph.D., in computer science . She has 29 years of teaching and research experience.six Candidates have completed Ph.D., under her guidance. She has authored numerous books, published 62 research articlesand conducted several conferences. She has also chaired sessions in international conferences,served as program committee member and chairman for Board of Studies in various colleges and universities.her area of specialisation includes Data mining, WBAN,Agent based computing and Advanced computer Networks.

G.Priyadharshini is a research scholar in the PG & Research department of computer science , Dr. Ambedkar Government Arts college, Chennai, India. She has completed her masters degree in Computer Applications and M.Phil., degree in computer science. She has 15 years of teaching experience and has published two research articles in International Journals. Her Area of specialisation includes Information Security, IOT, Cloud computing and software Engineering.