Network Security Firewall Technologies & IDS

Amr Mahmoud 17105415, Nada Hesham 17105766, Omnia Ahmed 17204229, Rana Mohamed 17105931

DR\Essam Hamed – ENG\Ahmed Gamal

Abstract

As internet has developed many fields like computer networks and network topologies. Network devices has become under threat of any attacks or malware. So, information security was a critical need. Although Firewall technology are used for network security, it cannot handle all the threats that are coming from unauthorized networks. There are different types of firewalls technology to develop a secured network. There are lots of researches covered firewall technology but the main purpose of this paper is to cover the firewall technologies such as, Packet Filtering, Stateful Inspection, Network Address Translation and Application-Level Gateway in order to prevent unauthorized accesses. As we said previously that firewall has limitations. IDS has immerged to provide real time detection of any attacks to build a secured network, the paper results show that both IDS and firewall technologies with types, functionalities and limitations and their integration can be a good idea to build a more protected network.

Keywords: Computer Networks, Attacks, Malware, Information Security, Firewall Technologies, Unauthorized Access, Firewall limitations, Internet Security, IDS.

Introduction

The emergence of networks and internet has revolutionized our life. As a result, many fields and areas like industry, business and other areas have developed so much as same as to the network related applications concerning WAN (ex: Internet) and LAN (ex: limited to organization/ Intranet) [1]. Internet usage in applications and network has brought so much easiness and effortlessness in configuring different networks, managing network applications and their internet connectivity. But with these perks regarding their usefulness, a lot of risks are caused by the internet like intrusions, vulnerabilities and software bugs which are increasing rapidly every day [3]. Since utilization of networks is a must for any business organization. So, business organization must take into consideration the privacy and protection of its sensitive data [1] from threats that would steal its data considering it is sensitive or not. Nowadays, Hackers or imposters try to make the default system abnormal system and exploit any vulnerability is the system [3]. In this paper, we will discuss solutions to the previous problems like firewall technologies and intrusion detection system. Ineffective security firewall and configurations can lead to vulnerabilities and software bugs [2]. Firewalls are mainly configured to protect the user's private network, prevent malicious users access and spread of malware and securing the network. We will discuss later the firewall mechanism and firewall technologies as considering Intrusion Detection system (IDS) that is used widely nowadays Features. Features are Packet filtering, Stateful inspection, Application-level gateways (proxies). IDS differs than firewall techniques like filtration, it doesn't filter traffic but it detects attack and alert the administrator. IDS is used for monitoring and firewall is used for providing protection to the private network form public network [1]. Dynamic inspection packet method is the best technology among the others firewall's technologies. It is a good or complete firewall system for network's traffic protection Usage.

Related Work

In January 2018, Gursewak Singh *et al* discusses some security issues and aspects as security mechanisms which are a must in any system like encryption, authentication, firewall types and technologies like packet filtering, Stateful Packet Inspection, ALG and NAT. he addresses some firewall limitations. Afterwards, IDS was explained briefly as its types and functions. How IDS mechanisms improve security of systems. At last, he concludes the combination of firewall and IDS can provide more security and protection to systems [1].

In April 2016, Mindo *et al* this paper discussed network security policy and its stages as initial stage, in preparation stage users' roles and responsibilities as well as privilege levels are defined. It should also clearly map the general user community, and the second stage of the policy entails conducting a risk analysis, (Low Risk, medium Risk and High Risk) and the last segment of the network security should entail creating a competent cross-functional security team that are familiar with the network security policy and have a great knowledge of the network topology, security design and implementation as well. Also discussed ISO-Functional models.

In April 2016, Nguyen discusses at first network security layers and how the intruder passes through many layers to steal information. Then, firewall technologies and their functionalities are explained. Later, he defined Network Security Policy, levels of security to manage network with useful way. At last, he addresses threats and their types and how they can be implemented into attacks as well as taking into consideration some malware like viruses, worms and trojans [3].

In June 2017, Richa Sharma et al classified Firewall is defined as the software and hardware or the combination of the both. To select firewall technic we are making a classification based on Features, Usage and Budgets. Features are (Packet filtering firewalls, Circuit-level gateway, Stateful inspection firewall, Application-level gateways (proxies), Multilayer inspection firewall, and Dynamic firewall). It is a good or complete firewall system for network's traffic protection Usage are (Software firewall, Hardware firewall). Budgets are (Commercial or paid firewall, Free or open-source firewall) [4].

In April 2016, S.C. Tharaka *et al* discusses, the most important aspect in network is security. Firewall security is one of the most important concepts of network security. Firewall can be hardware or software. There are firewall devices for network security and many installations software. The main use of firewall is to prevent unauthorized access or harmful events or it may slow down the spread. The firewall can block a traffic while allowing another traffic and this is often called filtering [5].

Related Studies

No.	Author(s)	Year	Title	Aim(s)	Method
1	Gursewak Singh & Bohar Singh	2018	NETWORK SECURITY TECHNOLOGY BASED ON FIREWALL AND INTRUSION DETECTION SYSTEM	Explains firewall technologies and IDS	Identify, extract And analyze Firewalls and IDS
2	Kirori Mindo, Caroline Sogomo & Nickson M. Karie	2016	Analysis of Network and Firewall Security Policies in Dynamic and Heterogeneous Networks	Discusses firewall security policy and review some network models	Archiving and reporting network security policies and ISO-FUNCTIONAL MODELS
3	Binh Nguyen	2016	Network Security and Firewall	Shows firewall technologies and network security polices	Processing and verifying firewalls, polices and attacks
4	Richa Sharma & Chandresh Parekh	2017	Firewalls: A Study and Its Classification	Classifies the firewall based on its features, usage and budget.	Archiving and reporting the different utilization for firewall
5	S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe & D. Dhammearatchi	2016	High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies	Discusses - packet filtering mechanism - firewall time-out - simple network topology	Research team has discussed a conceptualized paper on high secure network combining firewall technologies and capacity together.

Methodology

Firewall is basically a hardware or a software [4] that control the traffic between your network and other networks by filtering the ingoing and outgoing packets of information as a result of connection. For example, it allows network administrators to control activities on users' computers, filter and restrict data access and transfer data from inside out by observing. The incoming and outgoing network traffic and decides whether to accept traffic/communication or not based on security guidelines.it builds fence/gate protecting the user's network from any untrusted outside network [3].

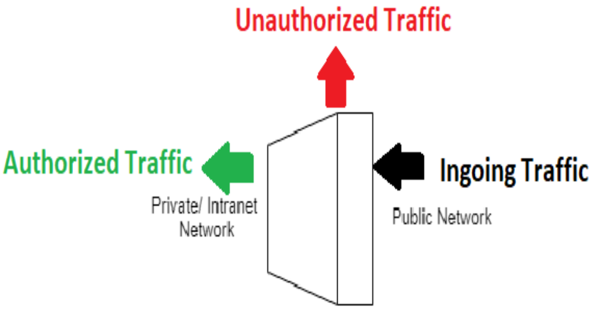


Figure 1: Firewall illustration

An efficient firewall is a must for any network to prevent from any network intrusions, threats or attacks. An attacker can penetrate the firewall and cause damages like placing malware [2].

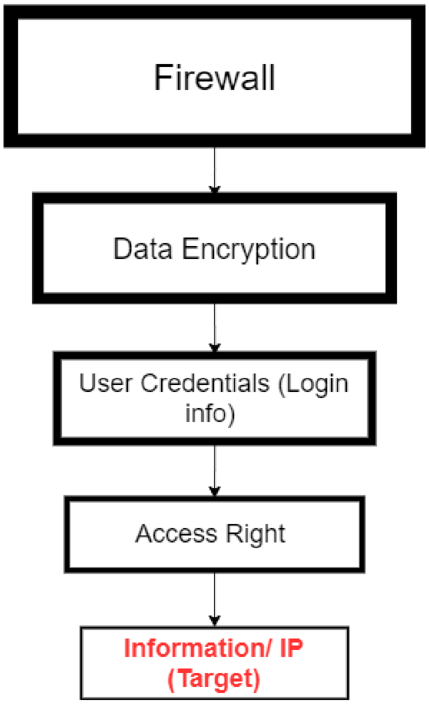


Figure 2: Network Security Layers

Those are the default commonly used layers in order to get user's information protected while transferring ingoing and outgoing traffic [3].

From outer to inner layer

1. **Firewall:** explained before as it is the outermost layer which filters ingoing and outgoing packets.
2. **Data Encryption:** Data must be encrypted with algorithms like Symmetric Encryption algorithms, Asymmetric Encryption algorithms and Hashing in order not to be visible to Intruders [1].

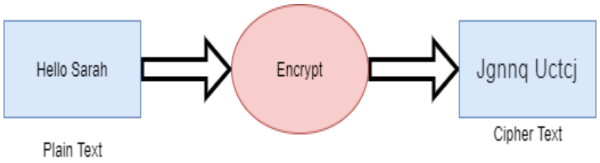


Figure 3: Caesar Cipher Encryption

3. **Login**: this layer limits system access and its resources only to its legitimate users.
4. **Access Right**: Controlling what can be accessed from resources and who can access those resources. Depending on users' prioritization from the manger to normal user (client) because a person like admin can control the users' activities.
5. **Target**: getting wanted information even if it is IP address.

Types of Firewall/ Firewall Technologies

1- **Packet filtering/ Stateless**: it is the Simplest type of firewalls as its technology filters quickly the packets based on many attributes (protocol, source IP, destination IP, source port and destination. port). It applies a set of rules to each packet if it matches these rules (Access Control List) and allowed to network without checking its contents, the firewall will accept the packet otherwise the packet will be discarded. This type of firewall is better configured to communication between "trusted" hosts because there can be malicious data tagged in the payload section of the packet if there is unauthenticated host in the communication. So, Packet filtering firewalls are low in security [4][1][5].

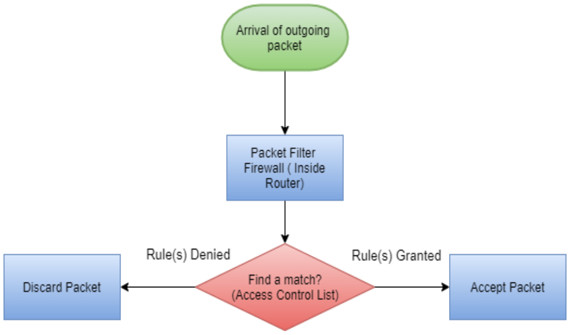

Arrival of outgoing packet
Packet Filter Firewall (Inside Router)
Rule(s) Denied
Rule(s) Granted
Discard Packet
Find a match? (Access Control List)
Accept Packet

Figure 4: Packet Filtering Mechanism

2- **Stateful inspection firewall**: This technology is the evolution of previous technology. Dynamically configure rule to the return traffic to come back. Stateful inspection, analyzing the packets by recording session attributes such as IP addresses and port numbers not only the header Information like the static packet filtering. So, it is dynamic packet filtering. It filters the traffic to check if the traffic I created from the initiation of the user or some intruders want to send malicious files to the user [3][1].

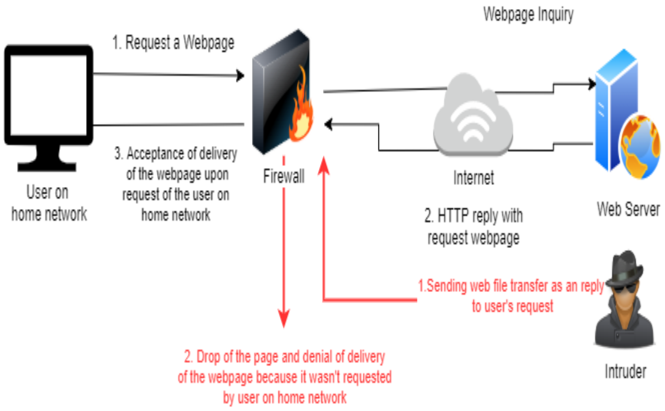

1. Request a Webpage
Webpage Inquiry
User on home network
3. Acceptance of delivery of the webpage upon request of the user on home network
Firewall
Internet
Web Server
2. HTTP reply with request webpage
1.Sending web file transfer as an reply to user's request
Intruder
2. Drop of the page and denial of delivery of the webpage because it wasn't requested by user on home network

Figure 4: Stateful inspection firewall illustration

3- **Network Address Translation (NAT):** this type of firewalls allows a network to assign a public address for internal node(s) inside a private network for communicating with outside host(s). Thus, the real IP addresses of those internal nodes are private or hidden to outside host(s). NAT does not grant any security aspects by itself but it helps to hide the internal network infrastructure and to force connections to go through a choke point which does the translation of addresses. The router sends modified packets by changing the source address of the packet to another valid address. As external host wants to send a packet. It will send it to the public address normally and the router will translate the destination address to the correct address of internal destination node [1].

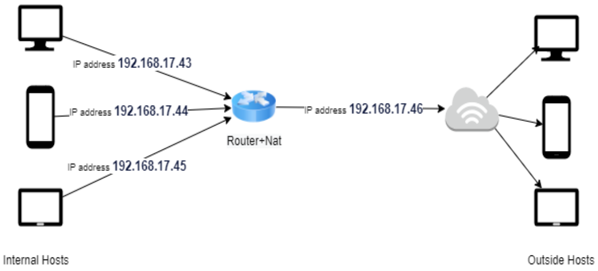


Figure 5: NAT firewall illustration

4- **Application-level gateways (ALG/ proxies)** is a firewall proxy or a firewall depends on proxy service method. Basically, it works at application layer of OSI model. The firewall filter only the packet to intended/ certain applications/ service with certain specifications. The mechanism is ALG acting as a bastion host/ proxy server which restricts the arrival of packets from the source. So, it can examine their payload, and then forward to destination. For example, if a user wants to send packets to a specific host, it communicates with proxy server with HTTP or TELNET and the proxy server will accept the packets and changes the ip address of those packets to its. By this way, the ip address of the internal user is hidden to the outside host(s) [3][4].

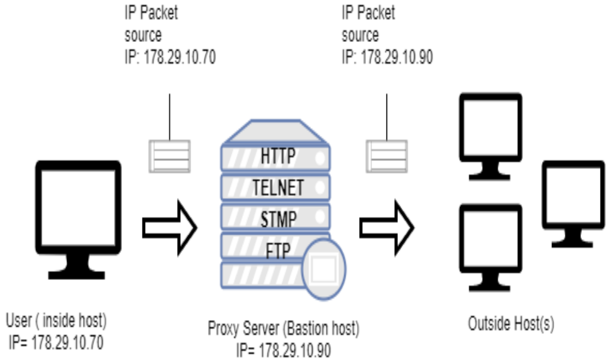


Figure 6: Proxy Server/ ALG Firewall Operation

IDS

Deploying systems with traditional defense didn't take the security as an essential fact because system with defense like that can be vulnerable when working in a different environment. So, intrusion detection system was taken into consideration. IDS can be hardware or software and its functionality is to monitor networks actively for detecting malicious activities and report them to system admin by alerting or by storing them into SIEM. Some of IDS's can respond and prevent attacks [1]. Basically, it is installed on user's computer of it is host-based or resided on the network if it is network-based. IDS fall into 2 categories which are

Signature-based intrusion detection system: stores every attack in a database by intruders because we can obtain signature form intruder's packets and compare this signature with the signatures that stored in the database or has been previously created.

In order to record any unwanted activity from attacker who previously attacked the system [1].

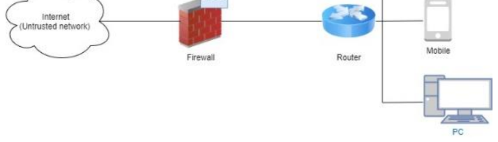
Anomaly-based detection system: it differs than the previous type because it doesn't depend on signature but it depends on rules or baseline. Baseline is considered to be the normal state of network. So, any activity lies outside the baseline, it is blocked automatically [1].

Discussion

With a firewall, the incoming and outgoing traffic will be filtered based on your firewall rules, so your system will not be able to be attacked at any time and your data will be secured. When Vulnerabilities are exploited, vulnerabilities make threats possible. If threat is carried, it will be considered an attack. There are many types of attacks that pose a risk to your system ex: IP address Spoofing: the intruder tries to send a packet using same as IP address of internal users as fake identity. Firewall can prevent this attack if it uses input filter to packets. Denial of service attacks: it is executed when floods of requests to host/server. That will affect system's availability resulting in overwhelming in host's capacity to reply to these requests [3].

An efficient firewall protects any network from intrusions, threats or attacks. An attacker can penetrate the firewall and cause damages like placing virus which is self-replicating to targeted folder or program in order to infect it but it is enabled by the user to be replicated [3].

Another damage like worms which are like viruses but worser because they can replicate themselves through the network to shut down it. It doesn't need to be enabled by the user. The last malicious program is the Trojan. Trojans are like backdoors that hide behind trusted applications. A good network infrastructure constructed with efficient firewall integrated with IDS to prevent any malicious activity [3].



Conclusion

As technology revolutionized our life as New network technologies and aspects have faced us with its issues. Old ways of securing and protecting data had been old fashioned and inefficient in facing huge/ fatal network issues such as threats, vulnerabilities or attacks. So, firewall and IDS are created to cope with this technology. Firewall technologies and an intrusion detection system help us from hackers who pose a threat to our data each firewall has its beneficial use but based on requirements of internet security policy. because particular firewall is used according to our utilization/ usage there are many types of firewall, each type does something different from the other from Packet filtering that it applies a set of rules for each packet if it matches certain criteria in order to be forwarded to another type which is Application-level gateways that examines payload, and then forward to destination. As IDS must be implemented in nowadays systems because it has become an essential part of any security system with its functionalities. Individual application of firewall or IDS is not enough to cope up with all security requirements but to improve security mainly for the network.

References

[1] Gursewak Singh et al, 2018. *NETWORK SECURITY TECHNOLOGY BASED ON FIREWALL AND INTRUSION DETECTION SYSTEM.* s.l.:s.n.

[2]Kirori Mindo et al, 2016. Analysis of Network and Firewall Security Policies in Dynamic and. p. 6.

[3]Nguyen et al, 2016. Network Security and Firewall. 29 April, p. 41.

[4]Richa Sharma et al, 2017. *Firewalls: A Study and Its Classification.* India: International Journal of Advanced Research.

[5]S.C. Tharaka et al, 2016. *High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies.* Sri Lanka: International Journal of Scientific and Research Publications.