High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies

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

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd

Abstract- This paper presents a detailed study of firewall technologies which are commonly used for network security. A firewall cannot handle all the destructive threats which are coming from unauthorized networks. Therefore, to develop a secured network different types of firewall technologies are used. Lot of researches have been done considering technologies of firewalls. The main purpose of this paper is to apply firewall capacity along with other firewall technologies such as packet filtering, network address translation, virtual private network and proxy services in order to prevent unauthorized accesses. Due to lack of many researches, related to firewall capacity and firewall technologies together. The research group focuses to build a more protected network by combining both firewall capacity and firewall technologies. The experiment results show the proposed idea good enough to build a secured network.

Index Terms- firewall technologies, firewall capacity, packet filtering, network address translation, virtual private network, proxy services

I. INTRODUCTION

Security is the most important aspect in a network. There are a lot of concepts for network security. Firewall is one of the most important concepts related to the network security. The term "firewall" was came to use in 1764, to describe walls which distinct the parts of a building most likely to have a fire from the rest of a structure. Firewall can be software or hardware. There is many installation software for network security; likewise, there are firewall devices for network security.

A firewall is designed in order to prevent or slow the spread of harmful events using firewall technologies to secure the network. Packet filtering, the firewall technologies that are currently existing can be named as Network addressing translation, Circuit-Level gateways, virtual private network, Proxy service, Application proxies and Application-Level gateway [1]. The firewall has a mechanism to allow some traffic to pass while blocking the other traffic (this is often called filtering). Most of the researches that have been done up to date focus on network security using firewall technologies. These researches focus on combination of few firewall technologies like packet filtering, Virtual Private Network and Network Address Translation. When consider about Network security one of the most important points that should be taken in to attention is the firewall capacity. Firewall behavior basically depends on the capacity. Firewalls with higher capacities are expensive. The proposed system will acquire a more secured network combining low capacity firewall and firewall technologies. The Packet filtering is referred to as static packet filtering, this method Controls the access to a network by analyzing the incoming and outgoing packets and letting them pass or uncertain them considered on the IP addresses of the source and destination. Packet filtering is one of the techniques, among many for implementing protected firewalls. The Network address translation is a methodology of remapping one IP address space into another protocol datagram packet header while they are in transit across a traffic routing device. A Circuit-Level gateway is a type of firewall technique. Circuit-Level gateways perform at the session layer of the OSI model or "shim-layer" between the application layer of the

TCP/IP stack. They monitor TCP handshaking between packets to determine whether a request session is legitimate. Create secure networks connection over a public network owned by a service provider is a virtual private network. Large corporations, educational institutions, and government agencies use virtual private network technology to enable remote users to securely connect to private network. A Proxy firewall is a network security system that prevent network resources by filtering messages at the application layer. An Application-Level gateway is firewall proxy which provide network security. It filters incoming node traffic to certain specifications which mean that only communicated network application data is filtered.

II. RELEVANT RESEARCH PAPERS

This research mainly defines about Network Address Translation (NAT) and Packet Filtering rules. Network Address Translation (NAT) is the process where a firewall assigns a public address to a computer or group of computers inside a private network. The main use of Network Address Translation (NAT) is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes. A process of packet filtering is controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP

addresses of the source and destination. Packet filtering is one technique among many for implementing security firewalls. But this paper is only focused about few firewall techniques, and it does not discuss about the firewall capacity. The firewall capacity exceeds large firewall should be replaced. So the cost will be high [2].

This research mentioned about how firewalls are used to protect resources from outside intruders and how Virtual Private Networks (VPN) enables to access the corporate network in a secure manner via non-secure public networks. A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. It uses data encryption and other security mechanisms to prevent unauthorized users from accessing data, and to ensure that data cannot be modified without detection as it flows through the Internet. It then uses the tunneling process to transport the encrypted data across the Internet. Tunneling is a mechanism for encapsulating one protocol in another protocol. VPNs reduce remote access costs by using public network resources. Including private networks, a VPN is inexpensive. This paper is focuses on only VPN technique which is including in firewall. But there are more firewall technologies to make more secure network [3].

This research mainly focuses on the packet filtering rules, advantages, and disadvantages of it. In packet filtering, each packet passing through a firewall is compared to a set of rules before it is allowed to pass through. Depending on the packet and the rule, firewall can drop the packet, forward it, or send a message to the resource. This paper is disadvantageous as it focuses on only one packet firewall technique. Therefore, they are not considered to be secure on their own. And also they cannot make any content-based decisions on packets. Testing the grant and deny rules is also difficult, which may leave the network vulnerable or incorrectly configured [4].

The authors of this research focuses on packet filtering, network address translation and application proxies. Network address translations are placed in the borders of stub network domain. For all routed data grams, it translates the local address into unique address and vice versa. Using application proxies, for each application, separate forwarding service must be provided. This paper introduces a framework in the form of waterfall model. And also it describes about the generalized concept of authenticated signaling. But this paper is disadvantageous as it focuses about only few firewall techniques, and it does not discuss about the firewall capacity. If the firewall capacity exceeds, large firewall should be replaced. So the cost will be high [5].

This research focus on a Method and apparatus for configuring a client to redirect requests to a caching proxy server based on a category ID with the request. A computer network including a client, at least one caching proxy server, and a destination computer is described. In a specific embodiment, a client computer may request particular types of information by including a category ID in request messages. In order to reduce network traffic, the destination computer may redirect the client's request messages to a caching proxy server, which is preferably located behind the same firewall or gateway as the client. The destination computer may initiate the redirection of client computer requests after receiving an HTTP proxy--GET request message from the client. The destination computer sends a message to the caching proxy server specifying the categories of request that the client computer will direct to the caching proxy server. The proxy server forwards this message to the client computer. The client computer uses the information contained in this message to direct requests messages to a specific caching proxy server based on a category ID. However, this research product is not covered in packet Filtering, Network Address Translation, Circuit-Level Gateways, Application Proxies, Application level Getaway arears [6]. D.Twum says that virtual Private Network technology allows remote network users to benefit from resources on a private network as if their host machines actually resided on the network. Each resource on a network may also have its own access control policies, which may be completely unrelated to network access. Thus users' access to a network does not guarantee their access to the sought resources. With the introduction of more complicated access privileges, such as delegated access, it is conceivable for a scenario to arise where a user can access a network remotely (because of direct permissions from the network administrator or by delegated permission) but cannot access any resources on the network. There is, therefore, a need for a network access control mechanism that understands the privileges of each remote network user on one hand, and the access control policies of various network resources on the other hand, and so can aid a remote user in accessing these resources based on the user's privileges. This research presents a software solution in the form of a centralized access control framework called an Access Control Service (ACS) that can grant remote users network presence and simultaneously aid them in accessing various network resources with varying access control policies. At the same time, the ACS provides a centralized framework for administrators to manage access to their resources. The ACS achieves these objectives using VPN technology, network address translation and by proxy various authentication protocols on behalf of remote users. However, this research product is not covered in packet Filtering, Network Address Translation, proxy Services, Application Proxies, Application level Getaway arears [7]. Wason T., Chandra A., focuses on network security according to a firewall policy. The advantage in this theory is Network Address Translation (NAT) which used to hide true addresses of protected hosts. The NAT function was developed to address IPv4 routing addresses that could be used or assigned to computers in order to

reduce the cost of obtaining public addresses for every computer. But this research does not concern about firewall capacity therefore in the high security firewall research it will concern about the firewall capacity which will help the people to choose the most suitable firewall to prevent network attacks [8].

This research mainly focuses on firewall techniques like packet filtering and circuit level gateways. Circuit level gateways monitor TCP handshaking between packets to determine whether a requested session is legitimate. In packet filtering only the authorized data packets are passed through the firewall. This research is disadvantageous as it only focuses about few firewall techniques. Therefore, high security firewall system will focus on having proxy services information packets would not pass through a proxy and proxy act as an intermediary computer. Therefore, this prevents direct connections and packet transfer between either sides of the firewall which makes harder for intruders to find the location of network where the packet is coming from [9].

Online examination system is used to provide exam online for remote candidates. The system is consisting of a web based server with a database facility. Database it contains User information and authentication for the Examination. Firewall technologies are used to make a secure system for online examination. Virtual Private Network (VPN) and NAT (Network Address Translation) these type of technologies is used to build this system. A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. In order to gain access to the private network, a user must be authenticated using a unique identification and a password. An authentication token is often used to gain access to a private network through a personal identification number (PIN) that a user must enter [10].

Sharma, Bhisham, and Karan Bajaj state that packet filtering is the main technology that this research focuses on in order to prevent unauthorized traffic form network. The filtering decision is taken according to a set of ordered filtering rules written based on predefined security policy requirements. This research mostly considers about traffic of network and how to make secure network without any unauthorized access [11].

This report will provide readers with a resource for understanding firewall design Principles used in network security. Firewalls fall into four broad categories: packet filters, circuit level Gateways, application level gateways and state full multilayer inspection firewalls. In a packet filtering firewall, each packet is compared to a set of rules before it is forwarded. The advantages of Packet filtering firewalls are low cost, have only a small effect on the network performance, and do not require client computers to be configured in any particular way. Circuit level gateways examine each connection setup to ensure that it follows legitimate TCP handshaking. Application level gateways Packets received or leaving cannot access services for which there is no proxy. The problem of this paper is that it does not focus on network capacity. So the performance will be decreased [12].

This research mainly focuses on the firewall capacity, advantages, and disadvantages of it. High firewall capacity helps the system to reduce the cost of replacing the low capacity. This paper is disadvantageous as it focuses on only one packet firewall technique. Therefore, they are not considered as a secured firewall. And also it may leave the network vulnerable or incorrectly configured. There are no any packet filtering techniques, which packet passing through a firewall is compared to a set of rules before it is allowed to pass through. So this a very big drawback for the system [13].

III. Solution

Research team has discussed a conceptualized paper on high secure network combining firewall technologies and capacity together. In a network, security is most important factor. In organizations, network is used to share their confidential information and secret methodologies. The lack of innovative security standards, hackers can hack the system and steal their private and confidential details. Therefore, most of the organizations use firewall as a security system. There are few firewall technologies to provide security in the network. Those firewall technologies are packet filtering, network address translation, circuit level gateways, virtual private network, proxy services, application proxies and application level gateways. Firewall capacity is one of the factors that should give the priority in order to speed the performance of the firewall.

Firewall performances are sometimes depending on the firewall capacity. High capacity firewalls can perform better. Most of high capacity firewall is expensive. The Proposed research will be focusing on high secured network using firewall capacity and combination of firewall technologies such as packet filtering, network address translation, virtual private network and proxy services. When advanced secured network is built using these technologies, the firewall capacity can be increased in order to increase the performance of the firewall, otherwise low capacity firewalls can slow down the performance. Then this will affect the security of network. Therefore, Research team decided to combine few firewall technologies together in order to improve the security of a particular network.

3.1. Reason *for consideration of these technologies*

Packet filtering technique, Network will identify packet which is authorized and other unauthorized packet will be dropped. Therefore, this technology is more important. Network address translation consider about public IP Addresses which are allocated in specific network, then hacker cannot take information using

unauthorized IP addresses. Virtual private network associates with private network and it helps to keep secure connection between sender and receiver. Proxy services, Proxies are mostly used to control, or monitor, outbound traffic. Some application proxies supply the requested data. This lowers bandwidth requirements and decreases the access the same data for the following user. It also gives indisputable evidence of what was transferred. These technologies are more important to build a secure network. Therefore, proposed research is based on these technologies and capacity of firewall.

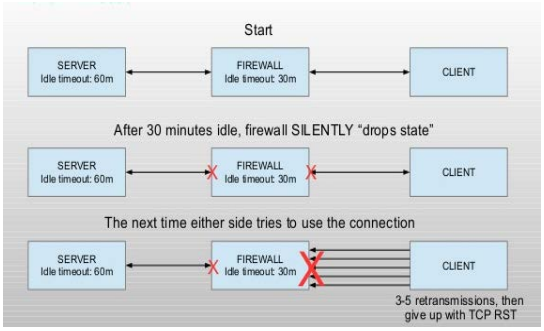

Figure 2: firewall time-out

Figure 2 represents the firewall time-out when firewall capacity is low.

IV. CONCLUSION

Firewall is a general technique which provide the authorize network access. There are many firewall techniques used to protect from unreliable accesses. Therefore, network should be configured in such a way that the network should not allow unauthorized users entering the network or accessing the information. The proposed research focuses on various technologies. packet filtering, Virtual Private Networks, Network Address Translation and firewall capacity. In packet filtering it focuses on passing or blocking packets at a network based on destination addresses, ports or protocols. Network Address Translation assigns a public address to a computer or group of computers inside a private network. It prevents from exceeding the number of public IP addresses an organization or a company must use for security purposes. Virtual Private Network is another technology that the research paper focuses, this

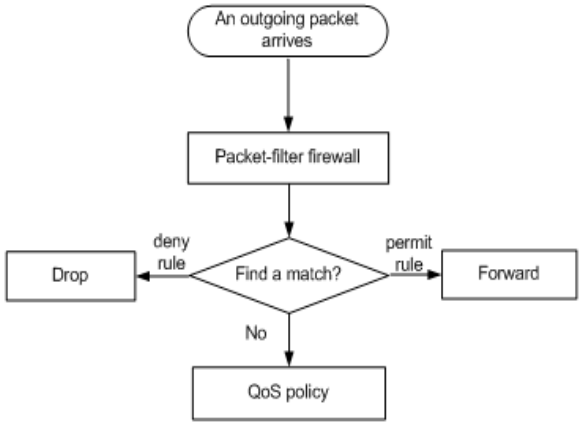

Figure 1:packet filtering mechanism

This figure 1 illustrates the mechanism of packet filtering technique.

3.2. Reason for consideration of the capacity of firewall

Firewall performance directly effects to network security and firewall performance depends on capacity of firewall. If firewall capacity high, it will give high performance. Therefore, research team selected firewall capacity for more secured network.

technique use encryption and other security mechanisms to make sure that only reliable users can access the network. The proxy server acts as a caching server to load the web page faster. The main technology focus in the research paper is the firewall capacity which helps to increase the performance of the firewall

Figure 3: simple network topology

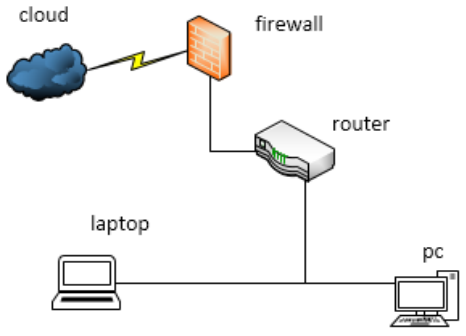

Figure 3 demonstrates a simple network topology which shows how the firewalls are connected in a network.

V. Future Work

The proposed research discusses about the advanced network security combining both firewall capacity and firewall technologies like packet filtering, Network Address Translation, Virtual Private Networks and Proxy Services. Due to Advancement of technology several cyber threats can occur in future. As a solution to overcome from these threats advanced security systems should be implemented. In future, researchers can focus on new aspects of firewall capacity in order to prevent cyber-attacks and including more firewall technologies. Thus, combining many technologies provides more effective access control and increases privacy.

References

[1] Imran, Mohammad, Abdulrahman Algamdi, and Bilal Ahmad. "Role Of Firewall Technolog In Network Security". International Journal of Innovations & Advancement in Computer Science 4.12(2016):8.Print.[04.02.2016].<https://www.researchgate.net/publication/292138198_Role_of_firewall_Technology_in_Network_Security>

[2] Taluja, Sachin, and Pradeep Kumar. “Network Security Using IP Firewalls". International Journal of Advanced Research in Computer Science and Software Engineering 2.8 (2012): 5. Print.[05.02.2016].<http://www.ijarcsse.com/docs/papers/8_August2012/Volume_2_issue_8/V2I800280.pdf >

[3] M .malik and R.pal, (2013),”impact of Firewall and VPN for WLAN”, International Journal of Advanced Research in Computer Science and Software Engineering,2.5.(2013) :5. Print [05.02.2016],<https://www.researchgate.net/publication/277567299_Impact_of_Firewall_and_VPN_for_securing_WLAN >

[4] Bhanot, Amit, and Leena jain. "Implementing Network Security Policies: Packet Filtering Mechanism". International Journal of Emerging Trends and Technology in computer Science 2.3 (2013): 3. Print. [05.02.2016].<http://www.ijettcs.org/Volume2Issue3/IJETTCS-2013-05-20-038.pdf>

[5] Ludwig, Christoph. "On The Modeling, Design, And Implementation of Firewall Technology". international journal of

[6] emerging trends & technology in computer science 5.4 (1997): 4. Print.[08.02.2016].<ftp://ftp.sdsc.edu/pub/mirrors/coast.cs.purdue.edu/pub/COAST/papers/Everything/schuba_phddis.pdf >

[7] PistriOttO, Joseph, and Katrina Montinola. "Method And Apparatus For Configuring A Client To Redirect Requests To A Caching Proxy Server Based On A Category ID With The Request". International Journal of Innovative Research in Technology 6.4 (2000): 10. Print.< https://docs.google.com/viewer?url=patentimages.storage.googleapis.com/pdfs/US6138162.pdf >

[8] Djin, Twum. "Managing Access Control In Virtual Private Networks". intrenational journal of Department of Computer Science, Dartmouth College 6.3 (2005): 6. Print.[04.02.2016].< http://www.cs.dartmouth.edu/reports/TR2005-544.pdf >

[9] Wason T., Chandra A.” Firewall Technology in Network Security”. International Journal of Innovative Research in Technology.4.3.(2006).6.print.[05.02.2016]. <http://www.engpaper.com/research-papercomputer-science-network-security.htm:>

[10] SingD.,SharmaR.,Etal,(2013),”Enhancement of Firewall Filtering Techniques”, International Journal of Emerging Trends and Technology in Computer Science.2.4.(2013): 5. Print [04.02.2016].<

[11] http://www.ijettcs.org/Volume2Issue4/IJETTCS-2013-08-16-090.pdf:>

[12] V, Selvi, Sankar R, and Umarani R. "The Design And Implementation Of On-Line Examination Using Firewall Security". IOSR Journal of Computer Engineering 16.6 (2016): 24. Print. [04.02.2016]. < http://www.iosrjournals.org/iosr-jce/papers/Vol16-issue6/Version-5/E016652024.pdf >

[13] Sharma, Bhisham, and Karan Bajaj. "Packet Filtering Using IP Tables In Linux". IJCSI International Journal of Computer Science Issues 8.4 (2011): 6. Print. [06.02.2016]. <http://ijcsi.org/papers/IJCSI-8-4-2-320-325.pdf >

[14] Woodall, Stephen. "Firewall Design Principles". international journal of Software Engineering6.4.(2004):8.Print.[02.02.2016].http://www4.ncsu.edu/~kksivara/sfwr4c03/projects/SteWoodall-Project.pdf

[15] MacVittie, Lori. "The Application Delivery Firewall Paradigm". international journal of emerging trends & technology in computer science 6.4 (2013): 8. Print. [04.02.2016]. < https://f5.com/resources/white-papers/the-application-delivery-firewall-paradigm >

Authors

First Author – S.C. Tharaka, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Second Author – R.L.C. Silva, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Third Author – S. Sharmila, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fourth Author – S.U.I. Silva, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Fifth Author – K.L.D.N. Liyanage, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Sixth Author – A.A.T.K.K. Amarasinghe, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd
Seventh Author – D. Dhammearatchi, Sri Lanka Institute of Information Technology Computing (Pvt) Ltd