Firewall: A Perimeter Security Solution

Rashmi B H, Usha C.R, Jayanth. P. Raj

Abstract: Firewalls today are an amalgamated part of security mechanisms of any institution or organization. Firewall is one of the important tools of network security system which is mainly used for the purpose of monitoring inbound and outbound packets. A firewall establishes a single point through which all the traffic passes. There are 2 types of firewall namely Network firewalls and Host-based firewalls. Management of network security and system security in today's complex environment is an open challenge. Many organizations and institutions have been enforced to strengthen the performance of an enterprise network by enhancing the features of firewall framework. In this paper, an insight into some of the existing features of the firewallis discussed and also an attempt has been made to show that the enhanced to the existing system policy portray different security mechanism in an organization and thus strengthening the capability of an enterprise network.

Index Terms: Firewalls, Active directories, Gateway Antivirus, Traffic shaper,SSL proxy, OpenVPN.

I. INTRODUCTION

The operation or capability of an Enterprise network is overblown not only, by the protocol specifications communication capabilities, and Firewall framework but also by its enactment and Traffic administration. Basically, Firewall is a key security solution which administers traffic in the network and also protects a network or system from unwarranted access.

A firewall is an important tool of network security system. Its main task is to have a track of ingoing and outgoing traffic. There were many generations of the firewall. The first generation of the firewall was Packet Filters. Packet Filter was the first type of firewall which looks at the ports and decides which packet should be allowed into the network or not. The aim of packet filters is to examine the packets which are transferred between computers on the internet. It consists of packet filter's set containing filtering rules, if the packet present here does not match the packet filter set, the packet will be discarded, if there is a match, the packet is allowed to pass. Second generation firewalls operate up to layer 4 of OSI model. These firewalls are stateful firewalls. These firewalls maintain the information of each state connected to it. Firewalls are often categorized as network based and host based.Network-based firewalls are the software appliance running on general purpose hardware which examines traffic between two or more network. A host-based firewall is the hardware solution which examines and filters the traffic in and out of the single machine.

Changing technology drives new requirement to enable security in an enterprise network. So to avoid certain vulnerable threats, existing firewall should be modified with certain new applications like firewall should act as a base for traffic monitoring. It should consist of features like packet filtering, web filtering, network address translation, protocol monitoring and VPN features. So by enhancing the firewall by these new features, the firewall should be in a position to monitor bad traffic, suspicious sites and should provide security at the gateway level. Understanding the concepts of IT perimeter security is one of the important tasks in the field of firewall and its policies.

Management of network security and system security in today's complex environment is an open challenge to both institution and as well as to an organization. Organizations are trying hard to improve existing firewall architecture in order to enforce security. With the advent of changing technology, certain changes to network security and policies should be enforced to avoid certain vulnerable threats. So large institutions and organizations should enhance the performance of security features in order to maintain security[1].

Network security basically consists of certainpolicies and practices to be imposed on the organization or an institution to enforce security. These policies and practices prevent and filters unwanted traffic, unauthorizedaccess, malicious contents entering into the network. The traditional firewalls lack these features. These firewalls are not able to restrict certain unwanted network, not able to filter protocols but only protect the criticalnetwork. So enhancement should be made to preserve security [2]

Firewall consists of access control lists. These access control lists consist of rules and policies to monitor incoming and outgoing traffic. These lists keep a track on the traffic which is being allowed or denied. Basically, these lists form a security policy to the firewall. Implementing and designing policies and rules to the firewall is a bit complex task. The administrator should be aware of new rules policies and rules and should update the firewall with the new requirements which seem to be error prone [3].

Some applications behave in an insecure manner when provided with untrusted SSL certificates. To avoid this, there is a method of informing the user about an SSL error and also send notifications as to which types of certificates should be accepted and presented during data encryption.To overcome this more secure TLS/SSL encryption should be carried out [5].

The need and scope of network security areunpredictable, as it prevents the network from illegitimateaccess, prevents from hacking and unauthorized access, Firewall acts a security perimeter. Firewall is a proxy server designed to monitor inbound and outbound traffic. But traditional firewalls find difficulty in protocol filtering, end-to-end data encryption etc. Therefore enhancement to this traditional model should be carried out in order to maintain security [6].Firewall are devices that control Incoming and outgoing traffic in an enterprise network having different security perspectives. Though Firewall monitors and controls internal and external traffic, thus enabling security, but threats are not always the same. With minimum applications, attacks can't be handled. The one main drawback of Firewall is that not much security is provided to the lower layers of network architecture. So to avoid these threats security should be provided to lower layers of network architecture also. To improve all these certain recommendations should be followed in a corporate network. First, important thing is that a firewall policy should be created to monitor inbound and outbound traffic, next is to gather all the requirements for the implementation of a firewall, thirdly create certain firewall rules that monitor firewall performance

II. ACTIVE DIRECTORY

Active directory is a central DB which stores all the information about all the people present in the organization. The structure of the active directory is as shown in Figure 1. It aims at manageability, provides security and allows interoperability. It creates a logical hierarchy and is highly secure. Many users can be added to a single domain. Active directory enforces AAA protocol. It stands for

- Authentication-It is the process of identifying someone's identity.
- Authorization-It is the process of verifying whether the authenticated person is accessing the resource or not.
- Accounting-It is the process of verifying whether both the authenticated and authorized person is accessing the resource or not.

Active directory has object types like users, groups, computer accounts and built in security accounts. Each and every object type has its own attribute defined by its type. For e.g.: if an object type by name user is considered, its attributes would be the first name, last name and contact address.

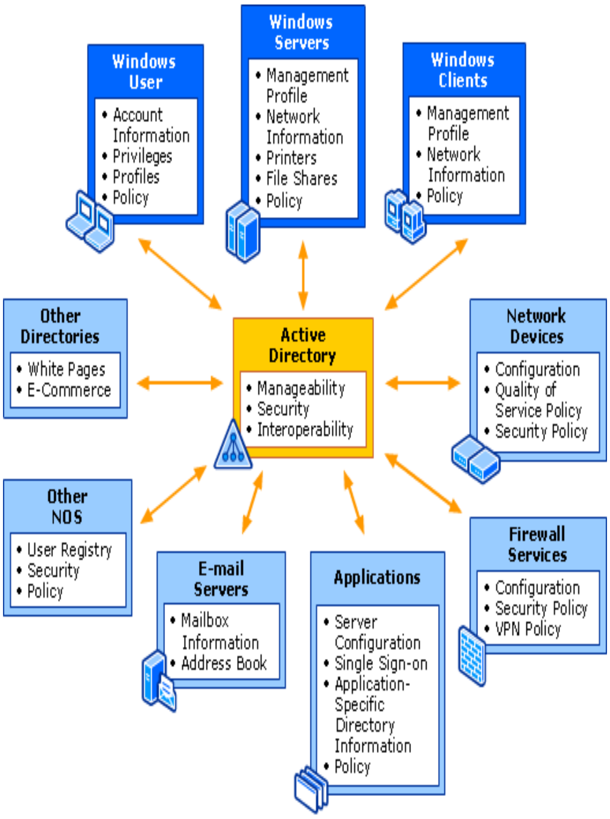

Figure 1: Structure of Active Directory.

III. FIREWALL

A firewall is a tool which monitors and filters ingoing and outgoing packets, thereby prioritizing network traffic. Firewalls act as Proxy server. They can act as both hardware and software system and protects and monitors the network from certain vulnerable threats and attacks. The main purpose of using a firewall in any institution or organization is that it protects a trusted network from the untrusted network by monitoring and filtering certain attacks and viruses. Firewall is associated with many characteristics for network protection. One of the main characteristics is that firewall provides various protection levels based on the location of the computer by applying various security levels in accordance with a particular type of network. The firewall provides protection to wireless networks (Wi-Fi) by carrying out intrusion detection method. When an intruder tries to access any unusual URL or a website, a message will be prompted with a warning as to block those sites immediately. A firewall protects the network against Hacking, which helps to access the computer to carry out certain actions. The firewall also blocks access to certain programs which seemed objectionable. Apart from all the above characteristics, one of the most important characteristics is that certain firewall policies and rules are defined in such a way which specifies the connections to be made, the ports to be allowed and the resources to which the access to be provided. Apart from these characteristics, the firewall is a bag of features used to strengthen the performance. Some of the features of the firewall are Light Squid, Squid, Squid guard, DMZ and WAN load balancer.

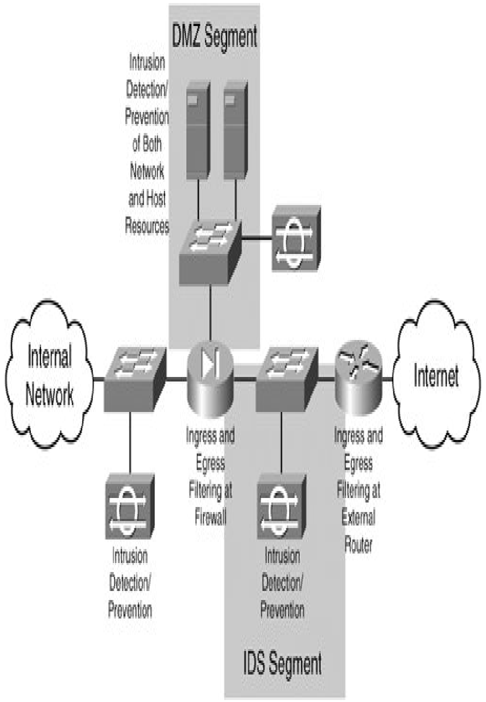
DMZ Segment
Intrusion Detection/ Prevention of Both Network and Host Resources
Internal Network
Internet
Ingress and Egress Filtering at Firewall
Ingress and Egress Filtering at External Router
Intrusion Detection/ Prevention
Intrusion Detection/ Prevention
IDS Segment

Figure 2: Firewall architecture

Light Squid is a fast log analyzer which generates the report on user log in HTML format. It provides an easy method of monitoring and examining internet usage. Before analyzing light squid, Squid logs should be stored in the default location. Squid is a web cache and a proxy server. Its main task is to cache the frequently used web pages. By caching it decreases bandwidth and increases response time.

Squid guard is a tool to carry out content filtering. This tool excludes access to certain URL and sites which seemed objectionable.WAN load balancer does the task of balancing the traffic among 2 WAN links.

Enhancement of firewall performance was carried out by introducing new features like OpenVPN, Gateway antivirus, Traffic shaper, Bandwidth limiter and SSL proxy. OpenVPN is used to implement VPN by creating point-to-point and secure site-to-site routed or bridged configurations and also provides remote access facilities.

Gateway antivirus is one of the unique features, which scans for threats and viruses at the router or gateway level and blocks them before they enter the network. Traffic shaping is also known as Packet shaping. The main task of traffic shaping is to manipulate and prioritize network traffic and to reduce the impact of heavy users affecting other users. Traffic shaper aims at saving bandwidth costs. Bandwidth limiters define the upload and download rates for the entire network. Bandwidth limiters manage bandwidth and prioritize network traffic.SSL proxy does the process of data encryption using TLS/SSL encryption.

IV. GATEWAY ANTIVIRUS

Gateway antivirus is one of the unique feature used to improve security in any organization or an institution. The main task of gateway antivirus is that it scans for viruses or threats at the router or gateway level and blocks those viruses or threats before they enter the network**.** It protects the network by proving information regarding Spyware and Malware threats. Antivirus blocks the data by file types also. The file types could be executables,media files or password attachments. Antivirus maintains a list of those things or people who are trustworthy and also has a list of things or people who are denied access. These lists are known as white and black lists respectively.

V. TRAFFIC SHAPER

Traffic shaping is also known as Packet shaping. It prioritizes network traffic by optimizing performance, improving latency and /or increasing bandwidth for some packets by reducing the impact of other kinds. There are two types of traffic shaping. The most common type is application-based traffic shaping wherein fingerprinting tools are used to identify the applications. Another type of traffic shaping is route-based traffic shaping,which is purely based on hop information. Traffic shaping is widely used in network traffic engineering, differentiated services and in various scheduling algorithms.

VI. SSL PROXY

Secure socket layer (SSL) is also called as Transport layer security (TLS). It is an application-level architecture that provides encryption services for the internet. SSL proxy ensures secure transmission of data between a client and a server by providing or ensuring privacy, authentication, confidentiality and data integrity. It is a transparent proxy which performs encryption and decryption between client and a server. SSL proxy expects certificates and key exchanges to happen properly. SSL proxy prevents unauthorized access.

VII. OpenVPN

OpenVPN is a software which implements Virtual private network (VPN) by creating secure point-to-point routed or bridged connections and also provides remote access facilities. It uses cryptographic algorithms namely SSL/TLS for encryption or decryption. OpenVPN allows a peer to communicate each other using well-defined certificates,pre-shared secret keys, and valid username/password. OpenVPN performs encryption using OpenSSL library and also adds an additional layer of security to the connection made using HMAC protocol. It performs authentication based on key exchange and certificates. OpenVPN acts as a custom security solution for the intruders who are trying to hack any confidential data in the system. OpenVPN runs over both Transmission control protocol(TCP) and user datagram protocol(UDP).

VIII. CONCLUSION

In this paper different characteristic of the firewall, techniques have been addressed. Apart from these characteristics, certain feature of the firewall has been addressed. The paper gives an idea on how these features could be used to strengthen the capability of firewall performance in an enterprise network. As and when the new technology emerges some more features can be undertaken in future to enhance the firewall performance.

IX. REFERENCES

[1] Kirori Mindo, Caroline Sogomo, Nickson M. Karie,” Analysis of Network and Firewall Security Policies in Dynamic and Heterogeneous Networks”, Vol.4.Mindo et al., International Journal of Advanced Research in Computer Science and Software Engineering 6(4), April- 2016, pp. 141-146.

[2] Jayshri V.Gaud, Mahip M.Bartere, “Data security based on LAN using distributed firewall”, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 386-391.

[3] Ameya Hanamsagar, Ninad Jane, Bhagyashree Borate, Aditi Wasvand, S.A. Darade,”Firewall anomaly management: A survey”,International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 18, November 2014.

[4] C.Socrates, P.M.Beulah Devamalar, R.Kannamma Sridharan,”Congestion control for packet switched networks”, International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.

[5] John Hubbard, Ken Weimer, Yu Chen,”A study of SSL proxy attacks on android and iOS mobile applications”, Jan 2014.

[6] Aakanksha Chopra, “Security issues of Firewall”, International Journal of P2P Network Trends and Technology (IJPTT) – Vol. 22 Number 1 January 2016.

[7] Manila Bohra, LaghviAloria, Neha Gupta,”Distributed firewall application for policy management and network security”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 2, April 2013.