DISTRIBUTED FIREWALL: A WAY OF DATA SECURITY IN LOCAL AREA NETWORK

Satinder[1], Vinay[2]

[1]*Assistant Professor (Extn.), Department of Computer Science,*
Govt. College For Women, Hisar, Haryana, INDIA
[2]*Computer Programmer, Computer Section, College of Basic Sciences & Humanities,*
CCS HAU, Hisar, Haryana, INDIA

ABSTRACT

Today, Computer and Internet network are essential part of our life. A number of personal transaction occur every second and computer network are mostly used only for transmission of information rather than processing. So, network security is essentialfor avert hacking of our confidential or important information. Network security can be attained by firewall. Firewall is a system or a group of system that implement a set of security rules to apply access control between two networks to protect inside network from outside network. In Short, we can say that, Firewall is a set of software programming and hardware device to secure host computer. A firewall is typically placed at the extremity of a system and act as filter for an illegitimate traffic. But, Conventional firewalls trust on the notions of restricted topology restriction and controlled entry points to apply traffic filtering.There are some problems for restricting the network topology i.e. End-to-End encryption problems, filtering of some protocols.Distributed firewallprotect from hackers attacks that originate from both the Internet and the internal network.Italso protect the client'scomputer and network's serversfrom unwanted hackers and intrusion.In this paper, we introduce the concept of distributed firewall. How to deal with the basic working, requirements and basic policies of distributed firewall?

Keywords*:: *Distributed Firewall, Network Security Techniques,Policy Distribution.

I. INTRODUCTION

In Today's world, Computer and Internet network are essential part of our life. A number of personal transaction occur every second and computer network are mostly used only for transmission of data and information rather than processing. So, network security is essential for avert hacking of our confidential or important data and information. Network security can be attained by firewall. A firewall is a hardware or set of instruction for permit or deny network transmissions based upon some protocols and regulation is frequently used to protect computer networks from unauthorized access while permitting constitutional communications to pass or during the sensitive data transmission. Traditional firewalls are devices often placed on the edge of the network that act as a bouncer allowing only certain types of traffic in and out of the network. Often called perimeter firewalls. They divide the network into two parts- trusted on one side and untrusted on the other. For this reason they depend heavily on the topology of the network.Conventional firewalls trust on the notions of restricted topology restriction and controlled entry points to apply traffic filtering. There are some problems for restricting the network topology i.e. End-to-End encryption problems, filtering of some protocols. Distributed firewalls are

used to allow enforcement of security policies on a network without restricting its topology on an inside or outside point of view. Distributed firewall protect from hackers attacks that originate from both the Internet and the internal network. It also protect the client's computer and network's servers from unwanted hackers and intrusion**.** Distributed firewall provide virtually unlimited scalability. They also solve the single point-of-failure problem furnish by the perimeter firewall. In Short, Distributed firewalls are host-terminal security software application that protect the entire network's servers and host-user machines against unwanted intrusion. They offer the advantage of filtering traffic from both the Internet and the internal network. This enables them to prevent hacking attacks that originate from both the Internet and the internal network. This is important because the most costly and destructive attacks still originate from within the organization.

II. BASICISSUES OF CONVENTION FIREWALL

A standard firewall is a set of elements, interposed between two networks that filter traffic between them according to some security code. There are some rules and codes to protect data from outside network. But not all the data are protected internally from insider of the network[1]

Some complications with the conventional firewalls that lead to Distributed Firewalls are as follows.

1) Depends on the network topology.

2) Do not secure the internal networks attack.

3) Do not handle FTP and Real Audio protocols.

4) There are also single level entry point and the failure of this leads to problems.

5) They do not stop "spoofed" transmissions.

6) Unable to logging all of the network's activity.

7) Unable to dynamically open and close their networking ports.

To solve these problems of the traditional firewall, the evolution of the distributed firewall comes into picture. They provide virtually unlimited scalability. Distributed firewalls are end-user-resident security software applications that protect the enterprise network's servers and host-user machines against unwanted invasion. They offer the leverage of filtering traffic from both the Internet and the internal network. This enables them to prevent hacking offense that originate from both the Internet and the internal network. This is important because the most destructive offense still originate from within the organization called inside offense[5].

III. A DISTRIBUTED FIREWALL DESIGN

Distributed firewall are host-resident security software applications that secure the enterprise network's servers and end-user machines against unwanted invasion. This endow them to prevent hacking attacks that originate from both the Internet and the internal network as given in the figure-1.They offer the feature of filtering traffic from both the Internet and the internal network. Usually deployed behind the traditional firewall, they give a second layer of security. Distributed firewalls secure the network by defending important network end-users, exactly where hackers want to invade.

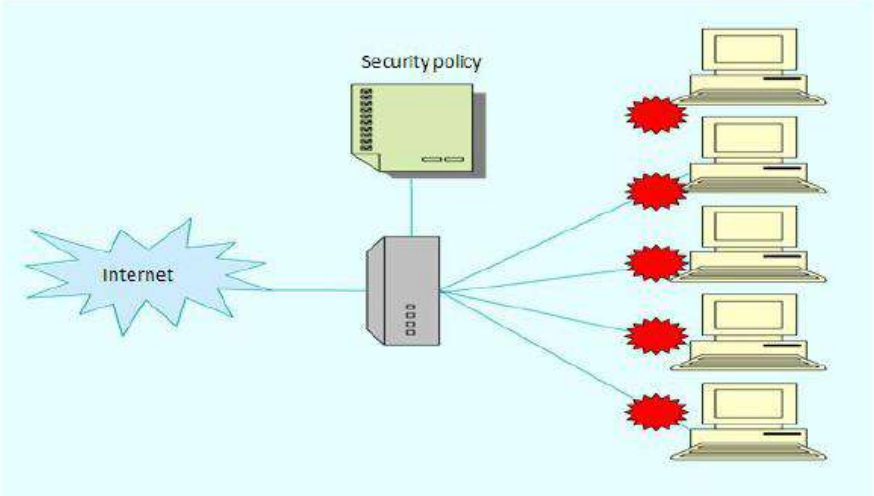

Figure.1 Distributed Firewall

The security policies are still defined centrally. The main motive with this approach is to retain the advantages of firewalls while clinching the disadvantages.They secure the individual machine in the same way that the perimeter firewall defend the overall network. The distributed firewall design is based on the idea forcing the policy rules at the endpoints rather than a single entry point to network.

IV. ARCHITECTURE OF DISTRIBUTED FIREWALLS

The network security policies are deployed in a decentralized way. The management is not allow the system administrators to set security policies from a server to host and fulfill the basic requirements of secure system and network administration. The concept of distributed firewalls, the network topological constraints are weakened and a decentralized use of traffic filters all over network. Distributed firewall system consists of four elemental parts:

4.1 The Management Center

This is responsible for the management of all end-users in the network, data security policy ordinance and distribution, log file receiving from the host network and analysis, invasion detection and so on.

4.2 Policy Actuator

Policy actuator is installed in each host network or every gateway to receive the data security policy provided by the management center, and implement the policy. It elucidate and runs the data security policy program. It is the program to defend the endpoint host networks, and it is mainly to recognize the function of the conventional firewall. Additionally, it is also to attain the functions of communicating with the management control center and implementing communication link request for the remote user-end.

4.3 Remote Endpoint Connectors

The remote endpoint connectors are the programs especially designed for the remote endpoint host networking, to prove their existence to Maintaining the Integrity of the Specifications. The template is used to modify your paper and text style. All paper margins, columns width, text fonts and line spaces are prescribed; please do not alter them. For example, the main margin in this template measures proportionately more than is conventional.

This dimensions and others are intended, using specifications that expect your paper as one part of the entire process, and not as an individual document. Please do not revise any of the current designations. Other hosts-users on a simple network, specially the internal host-point, request to establish communication with the internal endpoint. The network users use certificates to prove there authorized identity of the remote network server, while the certificate is sent to the endpoint by the management center through a security policy document mode, which can merge the remote endpoint connectors and the policy actuators. Thus, in one side the communication between the remote endpoint and the local endpoint is convenient, in the other side the remote endpoint can be provided security protects[1].

4.4 Log Server

The log server is important for the collection of the distinct events done in the whole network, such as basic networks protocol rule, log files, user login event logs, user Internet access logs, for audit analysis.

V. POLICIES

One of the most usually used term in case of network data security and in specially distributed firewall is policy. It is important to know about security policies. A “data security policy” defines the security rules of a system data and information[9]. Without a defined data security policy, there is no way to know what type of data access is allowed or disallowed. A simple example for a traditional firewall is:

- Allow all network connections to the web server.
- Deny all other unauthorized access.

The dissemination of the security policy can be distinct and different with the implementation. It can be directly pushed to endsystems, and pulled when vital.

5.1 Pull Technique

The end-user while booting up pings to the central management network server to check whether the central management network server status is up and active. It registers with the central management network server and requests for its policies which it should implement. The central management network server gives the host with its data security policies[8]. For example, a license server or a security clearance server can be asked if a certain communication should be allowed. A traditional firewall could do the same, but it shortage the important knowledge about the context of the request. End systems may know things like which files are included, and what their level of security. Such data and information could be carried over a network protocol, but only by adding complexity.

5.2 Push Technique

The push technique is engaged when the security policies are updated at the central management side by the network administrator and the end-users have to be updated instantly. This technology assure that the end-user/hosts always have the updated security policies at anytime[7]. The policy language defines which outbound and inbound network connections on any part of the network policy domains are allowed, and can influence the security policy decisions on any layer of the OSI network, being it at cancelling or passing certain packets or enforcing policies at the Application layer of OSI Network model.

VI. COMPONENT OF DISTRIBUTED FIREWALLS

- A central management system used for implementing the data security policies.
- A communication system to transmit these data security policies.
- Implementation of the security policies in the user end.

6.1 Central Management System

Central Management system, a component of distributed firewalls, makes it practical to protect desktops, enterprise-wide servers, Tablets, laptops, and workstations. Itgive greater control and efficiency and it reduce the maintenance costs of managing global security installations[2]. This feature addresses the need to maximize network security resources by enabling policies to be centrally configured, deployed, monitored, and updated. From a single workstation, distributed firewalls can be scanned to understand the current operating policy and to determine if updating is required.

6.2 Policy distribution

The distributed firewall policy distribution scheme should guarantee the integrity of the policy during transfer. This policy can be dissimilar and differ with the implementation[2]. The distribution of policy can be either straight pushed to end systems, or pulled when needed.

6.3 User-End Implementation

The security policies transmitted from the central management server have to be implemented by the user-end. The end-user part of the Distributed Firewall does give any administrative control for the network administrator to control the implementation of security policies. The end-user allows traffic based on the security rules it has implemented[2].

VII. ADVANTAGES OF DISTRIBUTED FIREWALLS

This is theessential advantage of distributed firewalls because they can secure hosts which are not within a network topology edge. The network security is no more dependents on network topology, it gives more flexibility in defining the data security policies. Distributed Firewall data Security policies can easily be extended to cover remote network hosts and networks whenever needed[6].

- The distributed firewalls network protect from hackers attacks that originate from both the Internet and the internal networkFiltering of some protocols like File Transfer Protocol are not easy for traditional firewall, on the other hand it is easy for distributed firewalls since all of the necessary information is available at the decision point, which is the end-user host in general[3].
- In standard firewalls there is an expectations that insiders are trustable. However this expectations is thesource of several networks issues. With the help of distributed firewall network the insiders are no longer trustable. Dividing network into parts having different security levels is much easier with distributed firewalls.
- Security policy rules are dispense and fixed on an as needed basis. Only the user-end that needs to communicate with the outside network should decide the properpolicy[1].

VIII. DISADVANTAGES OF DISTRIBUTED FIREWALLS

Acceptance of the network security policy for internal users is one of the major problem of the distributed firewalls. This issue speciallydone when each ending user host have the right of changing security policy. There can be some technologies tomake changing security policies harder but it is not totally impossible to save it. It is not so easy to implement an invasion detection system in a distributed firewall environment[4].

IX. CONCLUSION

The main objective of this paper to understand the concept of firewalls and distributed firewalls , providing the security during the transmission of data and information. Distributed Firewalls provide the secure environment for internet access. In this security policy is specified using KeyNotes policies and distributed to the users and hosts in the networks.So, with the help of distributed firewall concept we can achieve the followings goals,

- This Provide Complete data protection to the network.
- Distributed firewall allow or deny the network traffic meant for a particular system based on the policy it has to follow.
- Give Protection to the end-user of the networks from the inside and outside attacks.

X. FUTURE SCOPE

The update technology has many characteristics that, new policy is established and appended at the initiation of the present policy. New updated policy is created without any similar protocols. After the firewall updating and new configuration, the present implemented firewall has the uniqueness that the firewalls security policies protocols are based on the defined and develop rules'to manage the firewall to be utilized. For accuracy in detection and removing possible misconfiguration from the updated policy, it seems rectification algorithms, which determine potential errors, and also investigation in redundancy and shadowing is required.

REFERENCES

[1] http://www.seminarprojects.com/Thread-data-security-in-localnetworkusing-distributed-firewalls
[2] http://en.wikipedia.org/Distributed-firewall
[3] HiralB, Ravi S.Patel, JayeshA.Patel,"Approach of Data Security in Local Network using Distributed Firewalls", International Journal of P2P Network Trends and Technology-Volume1Issue3-2011.
[4] Sotiris Ioannidis, Angelos D. Keromytis, Steve M.Bellovin, Jona than M. Smith, "Implementing a Distributed Firewall" CCS '00, Athens, reece.
[5] Stevan M. Bellovin, "Distributed firewalls November 1999 issue
[6] W. R. Cheswick and S. M. Bellovin. "Firewalls and Internet Security": Repelling the Wily Hacker. Addison- Wesley, 1994.
[7] Robert Stapanek, "Distributed Firewalls", rost@cc.hut.fi,T-110.501 Seminar on Network Security, HUT TML 2001.
[8] Dr. Mustafa Hassan Dahshan "Security and Internet Protocol", Computer Engineering Department College of Computer and Information Sciences King Saud University [6] David W Chadwick, "Network Firewall Technologies", IS Institute , University of Salford, Salford, M5 4WT, England

[9] Anand Kumar "Data security in local networks using distributed firewalls" Cochin University of science and technology, August-2008.

[10] Robert Gwaltney, SANS Institute InFo Sec Reading Room, "Protecting the Next Generation Network – Distributed Firewalls", October 7, 2001.