Approach of Data Security in Local Network using Distributed Firewalls

Hiral B.Patel [1], Ravi S.Patel[2], Jayesh A.Patel[3]

[12]*BCA,Achraya Motibhai Patel Institute of Computer Studies*
[3]*Department of computerscience*
[123]*Ganpat University,Kherva*
[123]*Mehsana-Gozaria Highway*

***Abstract*—** firewall is a device or set of instruments designed to permit or deny network transmissions based upon a set of rules and regulation is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass or during the sensitive data transmission. Distributed firewalls allow enforcement of security policies on a network without restricting its topology on an inside or outside point of view. Use of a policy language and centralized delegating its semantics to all members of the networks domain support application of firewall technology for organizations, which network devices communicate over insecure channels and still allow a logical separation of hosts in- and outside the trusted domain. We introduce the general concepts of such distributed firewalls, its requirements and implications and introduce its suitability to common threats on the Internet, as well as give a short discussion on contemporary implementations.

***Keywords*—**Network Security, Security Policy, Pull technique, Push technique, Policy distribution

I. INTRODUCTION

Computers and Networking have become inseparable by now. A number of confidential transactions occur every second and today computers are used mostly for transmission rather than processing of data. So Network Security is needed to prevent hacking of data and to provide authenticated data transfer. Network Security can be achieved by Firewall. Conventional firewalls rely on the notions of restricted topology and controlled entry points to function. Restricting the network topology, difficulty in filtering of certain protocols, End-to-End encryption problems and few more problems lead to the evolution of Distributed Firewalls[1].

A distributed firewall is a mechanism to enforce a network domain security policy through the use of a policy language, a policy distribution scheme enabling policy control from a central point and certificates, enabling the identification of any member of the network policy domain. [1]

Distributed firewalls secure the network by protecting critical network endpoints, exactly where hackers want to penetrate. It filters traffic from both the Internet and the internal network because the most destructive and costly hacking attacks still originate from within the organization. They provide virtually unlimited scalability. In addition, they overcome the single point-of-failure problem presented by the perimeter firewall. [1].

Distributed firewalls are host-resident security software applications that protect the enterprise network's servers and end-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. [1]

II. ISSUES OF CONVENTION FIREWALLS

A firewall is a collection of components, interposed between two networks that filter traffic between them according to some security policy.

Some problems with the conventional firewalls that lead to Distributed Firewalls are as follows.
1) Depends on the topology of the network.
2) Do not protect networks from the internal attacks.
3) Unable to handle protocols like FTP and RealAudio.
4) Has single entry point and the failure of this leads to problems.
5) Unable to stop "spoofed" transmissions (i.e., using false source addresses).
6) Unable to log all of the network's activity and unable to dynamically open and close their networking ports. [1]

III. A DISTRIBUTED APPROACH TO FIREWALL DESIGN

As a result of dramatic increase in network complexity and development of new technologies like wireless networks and VPNs, it is not easy to maintain a fixed network topology anymore. Additionally, there are increasing user demands like mobility, security, performance and reliability. As a result of these and the disadvantages mentioned above, conventional firewalls have started to become inadequate. [6]

In order to remove such kind of problems, Bellovin and Ioannidis, et al. introduced the concept of distributed firewall. The distributed firewall design is based on the idea of enforcing the policy rules at the

endpoints rather than a single entry point to network. The security policies are still defined centrally. The aim with this approach is to retain the advantages of firewalls while resolving the disadvantages mentioned below [3]

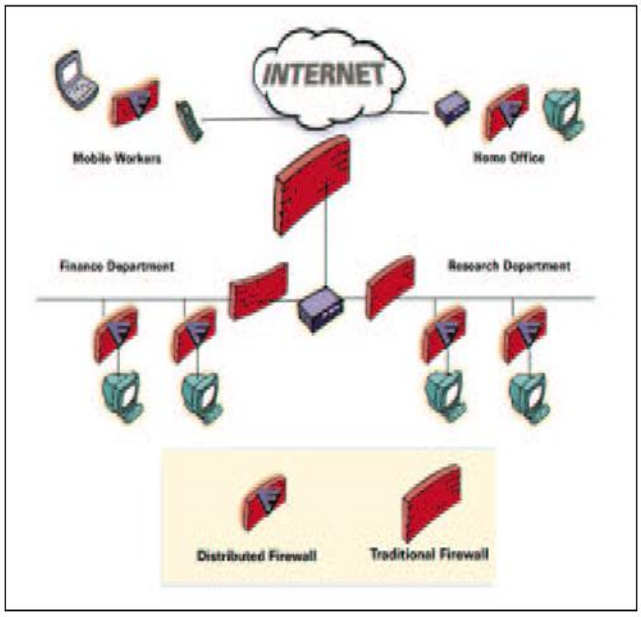

Figure 1. A distributed firewall architecture

There are three notions on which distributed firewalls based.
- Policy language: This is necessary to define what kind of connections are allowed or rejected.
- System management tools like Microsoft's SMS or ASD.
- Network level encryption mechanisms for TCP/IP such as IPSEC.

Basically, using these notions a distributed firewall system works as follows. The policy language is converted into an internal format using tool or a compiler. The system
management tool distributed this policy data to all of the hosts that are protected by the firewall. Then at each host, the incoming packets are accepted or rejected according to both
the security policy and cryptographic verification of each sender [3.6].

One of the critical points in a distributed firewall design is centralized management of the security policies. For such a large and complex system, centralized management is very important to provide consistency across all firewall devices in the system for enhanced security. Another critical point is to distribute policies in a secure way. To provide this, there is a need to use security services that guarantee the integrity, confidentially, authenticity of security policies [4, 6]

Policy Based Network Management (PBNM) is a new network management approach that abstracts the task of network management by providing a system wide approach to management and configuration. Opposing to traditional management systems that focus on device characteristics, PBNM treats the network as a whole and attempt to manage network as a single entity. PBNM performs this abstraction with the help of centralized storage, creation and management of network policies. This is very helpful to provide consistency, efficiency, reliability and a dynamic approach to system wide device configuration. Such kinds of things are very essential when managing security policies in a
Distributed firewall [4, 6].

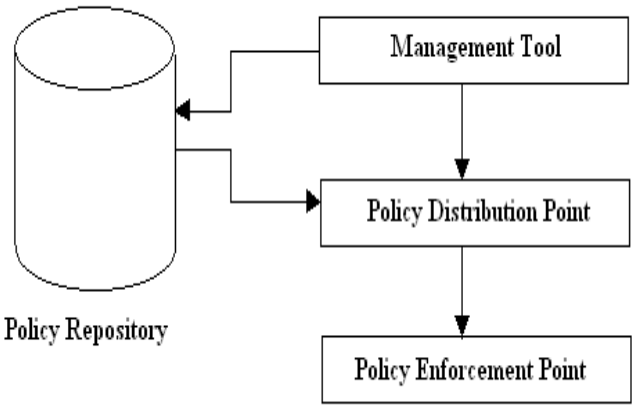

Figure 2. Architectural model of a PBNM system

IV. Advantages and Disadvantages of Distributed Firewalls

The introduction of distributed firewalls offered some solutions to the problems cannot be easily handled by conventional firewalls. The advantages of distributed firewalls
Can be stated as follows (Ioannidis, et al. 2000):
• Topological independence is one of the main advantages of distributed firewalls. Since network security no longer depends on network topology, it provides more flexibility in defining the security perimeter. Security perimeter can easily be extended to cover remote hosts and networks whenever required. [8]
• Opposing to conventional firewalls, network security is no more dependent on the single firewall so that problems like performance bottleneck and traffic congestion are resolved. Besides, the load on the traditional firewall is reduced since a large amount of filtering is performed at the end hosts.
• As mentioned earlier, filtering of certain protocols such as FTP are not so easy on a conventional firewall.

Such kind of a process is much easier on distributed firewalls since all of the required information is available at the decision point, which is the end host in general.

• The number of outgoing connections does not create so many difficulties in terms of network administration. Adding new links or removing existing links does not affect the network security. Similarly, backdoor connections that are created by insiders intentionally or inadvertently do not create new threats to network security in distributed firewalls.[6]

• As mentioned, in conventional firewalls there is an assumption on that insiders are trustable. However, this assumption is source of several problems. With the distributed firewall architectures, the insiders are no longer treated as
"unconditionally trusted". Dividing network into parts having different security levels is much easier with distributed firewalls.

• Security policy rules are distributed and established on an as-needed basis. Only the host that needs to communicate with the external network should determine the relevant policy. This approach dramatically eases the policy updating
process and does not require each firewall to maintain the complete policy set.

• End-to-end encryption is possible without affecting the network security in distributed firewall systems. In conventional firewalls, the use of end-to-end encryption was causing some problems in network security. On the other hand,
end-to-end encryption significantly improves the security of the distributed firewall.

On the other hand, there are some drawbacks of distributed firewalls that can be summarized as follows [5].

• Compliance of security policy for insiders is one of the major issues of distributed firewalls. This problem especially occurs when each ending host have the right of changing security policy. There can be some techniques to make modifying policies harder but it is not totally impossible to prevent it.

• It is not so easy to implement an intrusion detection system in a distributed firewall environment. It is possible to log suspicious connections on local server but these logs need to be collected and analyzed by security experts in central services.[6]

V. POLICIES

One of the most often used term in case of network security and in particular distributed firewall is policy. It is essential to know about policies. A "security policy" defines the security rules of a system. Without a defined security policy, there is no way to know what access is allowed or disallowed. A simple example for a firewall is:

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

The distribution of the policy can be different and varies with the implementation. It can be either directly pushed to end systems, or pulled when necessary.

A. Pull technique

The hosts while booting up pings to the central management server to check whether the central management server is up and active. It registers with the central management server and requests for its policies which it should implement. The central management server provides the host with its security policies. For example, a license server or a security clearance server can be asked if a certain communication should be permitted. A conventional firewall could do the same, but it lacks important knowledge about the context of the request. End systems may know things like which files are involved, and what their security levels might be. Such information could be carried over a network protocol, but only by adding complexity

B. Push technique

The push technique is employed when the policies are updated at the central management side by the network administrator and the hosts have to be updated immediately. This push technology ensures that the hosts always have the updated policies at anytime. The policy language defines which inbound and outbound connections on any component of the network policy domain are allowed, and can affect policy decisions on any layer of the network, being it at rejecting or passing certain packets or enforcing policies at the Application Layer.

VI. COMPONENTS OF A DISTRIBUTED FIREWALL

- A central management system for designing the policies.
- A transmission system to transmit these polices.
- Implementation of the designed policies in the client end.

A. Central management system

Central Management, a component of distributed firewalls, makes it practical to secure enterprise-wide servers, desktops, laptops, and workstations. Central management provides greater control and efficiency and it decreases the maintenance costs of managing global security installations. 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.

B. Policy distribution

The policy distribution scheme should guarantee the integrity of the policy during transfer. The distribution of the policy can be different and varies with the implementation. It can be either directly pushed to end systems, or pulled when necessary.

C. Host-end implementation

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

VII. CONCLUSION

The aim of this paper is the solution of computer crime means user can transfer his sensitive and important data or information that time firewalls and distributed firewalls provides the security during the data transmission. They provide the legal infrastructure for internet access. Firewalls provides the facility like only authentic user can access the computer or internet for his personal use they provides the authentication. In this paper we have tried to explain or prove the internet problems and solution of that problem with the help of distributed firewalls. Its also called filtering process. Firewalls is useful in many place like college or any institution for data security or network security purpose.so,its our solo paper for trying to awareness and provides the solution for networking through the distributed firewalls.

VIII. ACKNOWLEDGMENT

First and foremost we want to thank my ph.d. Guide Dr.Dhaval Kathiriya sir. We appreciate all his contributions of time,ideas,and funding to make my research paper. I am also thankful for the excellent example given by our dean Prof. Satyen Parikh sir who is successful person in academia.

IX.REFERENCES

[1] http://www.seminarprojects.com/Thread-data-security-in-local-network-using-distributed-firewalls
[2] http://en.wikipedia.org
[3] Bellovin, S. M. 1999. Distributed Firewalls.
[4] Gatus, G. E. P., Safavi-Naini, R. and Willy Susilo. 2004. Policy Distribution Using COPSPR in a Distributed Firewall. In Australian Telecommunication Networks and Applications Conference..
[5] Li, Wei. 2000. Distributed Firewall. GeoInformatica. 4(3):253
[6] Oguzhan ÇAKI, March 2008 ,Thesis on "ACCESS MONITORING SYSTEM FOR DISTRIBUTED FIREWALL POLICIES"
[7] Robert Stepanek, Distributed Firewalls In Article In T-110.501 Seminar on Network security 2001
[8] Yunus ERDOĞAN,November 2008,Thesis on "DEVELOPMENT OF A DISTRIBUTED FIREWALL ADMINISTRATION TOOL"