Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.386 – 391

RESEARCH ARTICLE

DATA SECURITY BASED ON LAN USING DISTRIBUTED FIREWALL

Jayshri V.Gaud[1], Mahip M.Bartere[2]

[1]Department of Computer Science & Amravati University, India

[2]Department of Computer Science & Amravati University, India

[1] jayshreegaud@gmail.com; [2] mahip.bartere@raisoni.net

Abstract— ***Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. In most of the systems, the network security is achieved by firewall and acts as a filter for unauthorized traffic. But there are some problems with these traditional firewalls like they rely on the notation of restricted topology and controlled entry points to function. Restricting the network topology, difficulty in filtering of certain protocols, end-to-end encryption problem and few more problems lead to the evolution of Distributed Firewalls. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. This paper is a survey paper, dealing with the general concepts 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. A distributed firewall gives complete security to the network.***

Keywords— Network Security; Pull technique; Push technique; Policy; Distributed Firewall

I. INTRODUCTION

It is virtually impossible to compete in today's fast-paced business environment without connecting your private network to the public Internet. Employees need to rapidly access and share information with partners, customers and the world at large if you are to stay ahead of the competition. Unfortunately, such connectivity provides an easy path for untrusted parties on the outside to penetrate a company's private network and access or tamper with internal information and resources. Lots of data are getting transferred through it; one can connect any computer in the world to any other computer located apart from each other. This is a great advantage for individual and corporate as well. But in this case, one should need the secure transmission of the data, by the concept of Network Security, which involves the corrective action taken to Ease of Use protect from the viruses, hacking and

unauthorized access of the data. It is a Network Security needed to prevent hacking of data and to provide authenticated data transfer.Network security is achieved by firewall.A Firewall is a collection of components, which are situated between two networks that filters traffic between them by means of some security policies. A Firewall can be an effective means of protecting a local system or network systems from network based security threats while at the same time affording access to the outside world through wide area networks and the Internet. 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. Moreover, firewalls are a mechanism for policy control. That is they permit a sites administrator to set a policy on external access. Just as file permissions enforce an internal security policy, a firewall can enforce an external security policy.

The solution to this growing problem will never be found by simply improving the security technology of traditional firewall products. What's needed is an entirely new model of perimeter security that recognizes the strengths of the firewall as an enforcement point, and then empowers it to "actively" communicate with the rest of the network, responding to new attacks and modifying security measures accordingly. What is required is a distributed firewall system that integrates and prevents security breaches both inside and outside the network.

II. Conventional Firewall

A firewall is system or group of system (router, proxy, or gateway) that implements a set of security rules to enforce access control between two networks to protect "inside" network from "outside network. It may be a hardware device or a software program running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to. A firewall is essentially a security enforcement point that separates a trusted network from an untrusted one. Firewalls screen all connections between two networks, determining which traffic should be allowed and which should be disallowed based on some form of security policy decisions determined in advanced by the security administrator.Conventional firewalls are devices often placed on the edge of the network that act as a bouncer. The firewall is used to enforce a central policy of what traffic is allowed in and out of the network. When traffic flows through the firewall it is evaluated by a set of rules based on ip address, port, etc. and either allowed or denied. All traffic entering or leaving the network must pass through this point. This requirement itself is often one of the downfalls of the firewall. For example, users might go around the firewall by using a modem or some other connection to the Internet. Another problem is encrypted tunnels, which provide a hole through the firewall where the traffic isn't evaluated and flows freely. Some problems with standard firewall as follows.

- Depends on the topology of the network.
- Do not protect networks from the internal attacks.
- Unable to handle protocols like FTP and RealAudio.
- Has single entry point and the failure of this leads to problems.
- Unable to stop spoofed transmissions (i.e., using false source addresses).
- Unable to log all of the network's activity and unable to dynamically open and close the networking ports.

To solve these problems of the firewall the evolution of the distributed firewall comes into picture. In the distributed firewall scheme, policy is still centrally defined: enforcement, however takes place on each endpoints. Distributed firewalls allow enforcement of security policies on a network without restricting its topology on an inside or outside point of view. Distributed firewall overcomes these problems with the conventional firewall. They offer the advantage of filtering traffic from both the Internet and the internal network.

III. Distributed Firewall

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. They are like personal firewalls except they offer several important advantages like central management, logging, and in some cases, access-control granularity. These features are necessary to implement corporate security policies in larger enterprises. Policies can be defined and pushed out on an enterprise-wide basis. A feature of distributed firewalls is centralized management. The ability to populate servers and end-users machines, to configure and "push out" consistent security policies helps to maximize limited resources.

The ability to gather reports and maintain updates centrally makes distributed security practical. Distributed firewalls help in two ways. Remote end-user machines can be secured. Secondly, they secure critical servers on the network preventing intrusion by malicious code and "jailing" other such code by not letting the protected server be used as a launch pad for expanded attacks.

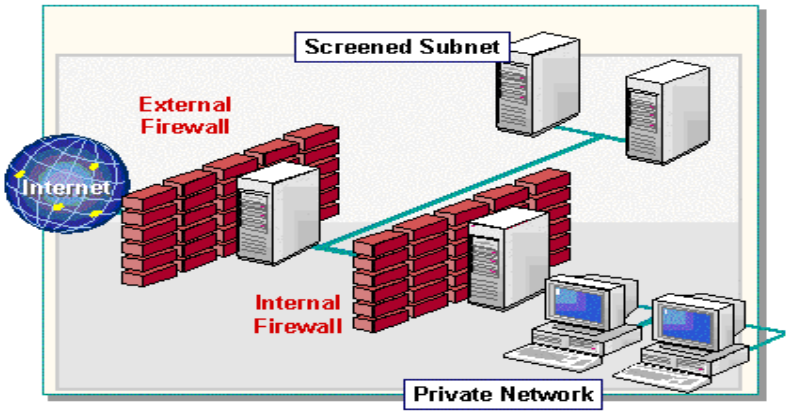

Fig.1 Example of Distributed Firewall

Distributed, host-resident firewalls prevent the hacking of both the PC and its use as an entry point into the enterprise network. A compromised PC can make the whole network vulnerable to attacks. The hacker can penetrate the enterprise network uncontested and steal or corrupt corporate assets. Unlike traditional firewalls, distributed firewalls are not placed in one location. As the name implies, the distributed firewall is installed throughout the network to all endpoints. Distributed firewalls are based on three main points.

A. *Policy Language*

The policy language is used to create polices for each of the firewalls. These policies are the collection of rules, which direct the firewall in how to evaluate the network traffic.

B. *System Management Tools*

The system management tools are used to distribute the policy to the firewalls and to collect logging and reporting information.

C.*IPSEC*

IPSEC provides network-level encryption used to secure network traffic and the transmission of policies. It also provides a more important function of providing a way to cryptographically verify the sender of information. Senders can then be uniquely verified by their certificate. Cryptography is the practice and study of techniques for secure communication in the presence of third parties .More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation**.**

IV. Components of Distributed Firewall

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.

V. Architecture of Distributed Firewall

Distributed Firewall Administration Architecture based on hierarchically organized distributed firewall system. The domain statement has a domain firewall which is standing on the domain entrance and protects the entire domain according to the organizational policy. According to the network model there are subnets available and connected to the domain firewall. Each subnet has a subnet firewall which is located on the subnet entrance. Purpose of the subnet firewall is same as the domain firewall. Every subnet may have different number of personal firewall; this personal firewall can control their network traffic. In addition subnet firewall may have child firewall which type can be subnet firewall. Communication scheme between these firewall nodes in the system as follows: personal firewall nodes has to maintain local rule base to store rules. They are responsible to enforce the local policy.
When personal firewall performs any operations such as insert, delete policy rule they have to propagate to their Subnet firewall. Subnet firewalls can communicate to all of the nodes inside that subnet but they cannot communicate to another subnet firewall at the same level. Similarly, a domain firewall can communicate to any other nodes in that domain. The communication between a domain firewall and leaf firewall is possible with the help of the subnet firewalls. Communication request of the domain firewall is received by the leaf level firewall via the subnet firewall.

VI. Working

Most distributed firewalls run in kernel mode and sit at the bottom of the OSI stack. The firewall evaluates all network traffic whether it is from the Internet or the internal network. This protects the system much in the same ways as traditional firewall protects the network. After the firewall is installed on all network endpoints, a central policy is developed. This policy is written using the policy language and then compiled in a format to be transferred to each firewall. The system management tools are then used to transfer the policy to each firewall. Because the firewalls are in different locations throughout the network and may be on a machine that changes locations, they cannot depend on the network topology to determine the sender of the network traffic. For this they use the certificates provide by IPSEC. These certificates uniquely identify the sender and don't depend on the network topology. The firewall then evaluates the traffic based on the central policy and decides to allow or deny it. The firewall can also then transfer logging information to a central location where it can be used for reporting.

VII. 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 any time. 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.

VIII. Advantages of Distributed Firewall

- This is the most important advantage of distributed firewalls because they can protect hosts that are not within a topology boundary. Since network security is no more dependent 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.
- Filtering of certain protocols such as FTP 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.
- 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.
- 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.
- End to end encryption is possible without affecting the network security in distributed firewall system.

IX. Disadvantages of Distributed Firewall

- Intrusion detection systems are less effective with distributed firewalls because complete network traffic is not on the single point.
- Compliance of the security policy for insiders is one of the major issues of the 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.

X. Conclusion

As networks continue to change and expand new tools are needed to keep them secure. Distributed firewalls take a new approach by securing every host on the network. They also have no trouble handling the changing topology of today's networks. This makes them a perfect match for telecommuters that work from remote locations and often use a VPN to connect to the corporate network. As they continue to develop, new features will be added that will only increase their security and ease of use. Distributed firewalls just may be the tool to secure next generation networks.

ACKNOWEDGEMENT

I would like to thank to all the people those who have help me to give the knowledge about these research papers and I thankful to my guide with whose guidance I would have completed my research paper and make it to published, finally I like to thank to all the website and IEEE paper which I have gone through and have refer to create my research paper successful.

REFERENCES

[1] http://www.seminarprojects.com/*Thread-datasecurity-in-localnetwork-using-distributed-Firewalls*
[2] http://en.wikipedia.org
[3] Hiral B .Patel, Ravi S. Patel, Jayesh A. Patel, "*Approach of Data Security in Local Network using Distributed Firewalls*", International Journal of P2P Network Trends and Technology Volume1Issue3-2011.
[4] Atul Kahate, "*Cryptography and Network Security*", ISBN-13: 978-0-07-064823-4, ISBN-10:0-07-064823-9, McGraw Hill Higher Education.
[5] Robert Stepanek, Distributed Firewalls In Article In T-110.501Seminar on Network security 2001
[6] Ioannidis, S. and Keromytis, A.D., and Bellovin, S.M. and J.M. Smith, "*Implementing a Distributed Firewall*", Proceedings of Computer and Communications Security (CCS), pp. 190-199[Robert Stepanek, "*Distributed Firewalls*", rost@cc.hut.fi, T-110.501 Seminar on Network Security, HUTTML 2001.
[7] Dr. Mostafa Hassan Dahshan "*Security and Internet Protocol*", Computer Engineering Department College of Computer and Information Sciences King Saud University mdahshan@ccis.ksu.edu.sa
[8] Anand Kumar "*Data security in local networks using distributed firewalls*", Cochin University of science and technology, August-2008.
[9] Robert Gwaltney, SANS Institute InfoSec Reading Room, "*Protecting the Next Generation Network -Distributed Firewalls*", October 7, 2001.
[10] Lane Thames, "*GLOBALIZING INTERNET SECURITY WITH A DISTRIBUTED FIREWALL AND ACTIVE RESPONSE ARCHITECTURE*", April 2008.
[11] Hiral B.Patel, Ravi S. Patel, Jayesh A. Patel, "*Approach of Data Security in Local Network using Distributed firewall".*
[12] Ioannidis, S. and Keromytis, A.D., and Bellovin, S.M. and J.M. Smith, "*Implementing a Distributed Firewall*", Proceedings of Computer and Communications Security (CCS), pp. 190–199, November 2000, Athens, Greece.
[13] Sneha Sahare, Mamta Joshi, Manish Gehlot "*A Survey paper: Data Security in Local Networks Using Distributed Firewall*" ISSN :0975-3397 Vol. 4 No. 09 Sep 2012, 1617
[14]Rajendra Rathod,"*Roll of Distributed Firewalls in Local Network for Data Security*" India. Vol. 6, No.2, Apr 2013 ISSN: 0974-1011 (Open Access).s

