Survey on Roll Of Distributed Firewalls In Local Network For Data Security Distributed Firewall

Mr.N.Karthick[1], Mrs.A.Kanimozhi[2]
[1, 2] Assistant professor, Dept of Computer Science
[1, 2] VLB Janakiammal College of Arts and Science, Kovaipudur, Coimbatore-641042.

Abstract- *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. 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. This paper is a survey paper, dealing with the general concepts such distributed firewalls, its requirements and research introduce, its suitability to common threats on the Internet, as well as give a short discussion on contemporary implementations that a distributed firewall gives complete security to the network.*

Keywords- Network Security, Pull technique, Push Technique, Policy, Distributed Firewall

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. It needed to involves the corrective action taken to ease of use protect from the viruses, prevent hacking of data and to provide authenticated data transfer. Firewall is a device or set of instruments designed to permit or deny network transmissions based upon a set of rules and regulations which are frequently used to protect networks from unauthorized access while permitting legitimate communications to pass or during the sensitive data transmission and it 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.
(Pritish A. Tijare et.al, 2014).

II. AN OVERVIEW OF FIREWALL

2.1 Firewall

A firewall is a system or group of systems (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 un-trusted 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. (Jayshri V.Gaud et.al, 2014)

2.2 Conventional firewalls

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.

2.3 Conventional firewalls Drawbacks.

- Depends on the topology of the network.
- Do not protect networks from the internal attacks.
- Firewalls can become a bottleneck
- Multiple entry points make firewalls hard to manage

- Unable to handle protocols like FTP and Real-Audio.ingle points of access make firewalls hard to manage.
- 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.

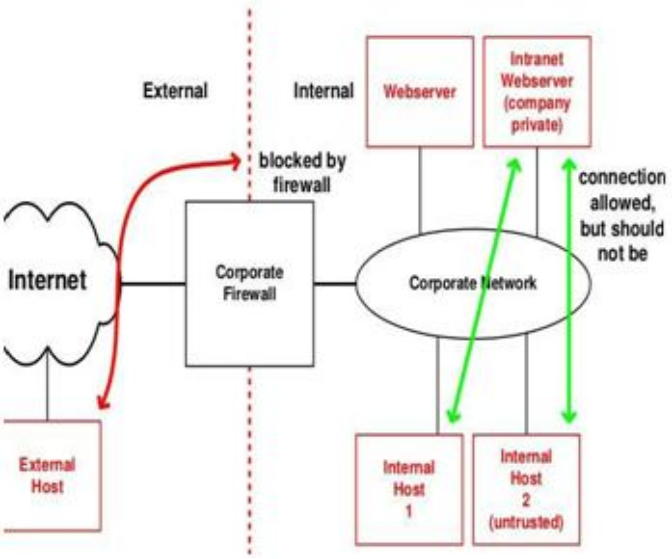

Figure 1 Standard firewall example, connection to intranet

III. DISTRIBUTED FIREWALL

3.1 Distributed firewall concepts

Distributed firewalls are host-resident security software applications that protect the enterprise network's servers and end-user machines against unwanted Intrusion and secure the network by protecting critical points, exactly where hackers want to penetrate. 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.

Distributed firewalls overcome the single point-of-failure problem presented by the firewall. 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. As the name implies, the distributed firewall is installed throughout the network to all endpoints. (Sotiris Ioannidis,et.al,2013)

3.2 Basis of distributed firewalls

Distributed firewalls are based on three main points.

- **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.
- **System Management Tools:** The system management tools are used to distribute the policy to the firewalls and to collect logging and reporting information.
- **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. 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**.**

3.3 Components of distributed firewall

There are three components of distributed firewall.

i. **Policy language:** Policy language used to create policies for each firewall. These policies are the collections of rules, which guide the firewall for evaluating the network traffic and also defines which inbound and outbound connections are allowed or rejected.

ii. **Policy distribution scheme:** Policy distribution scheme is used to enable policy control from central point. This policy is consulted before processing the incoming or outgoing messages. It should guarantee the integrity of the policy during transfer. It can be either directly pushed to end systems, or pulled when necessary with the implementation.

iii. **Certificate:** Certificate enables making decisions without knowledge of the physical location of the host. There may be the chance of using IP address for host identification by the DFW, it is preferred to use certificate to identify hosts. IPSec provides cryptographic certificates, unlike IP address which can be easily spoofed, the digital certificate is much

more secure and the authentication of certificate is not easily forged.

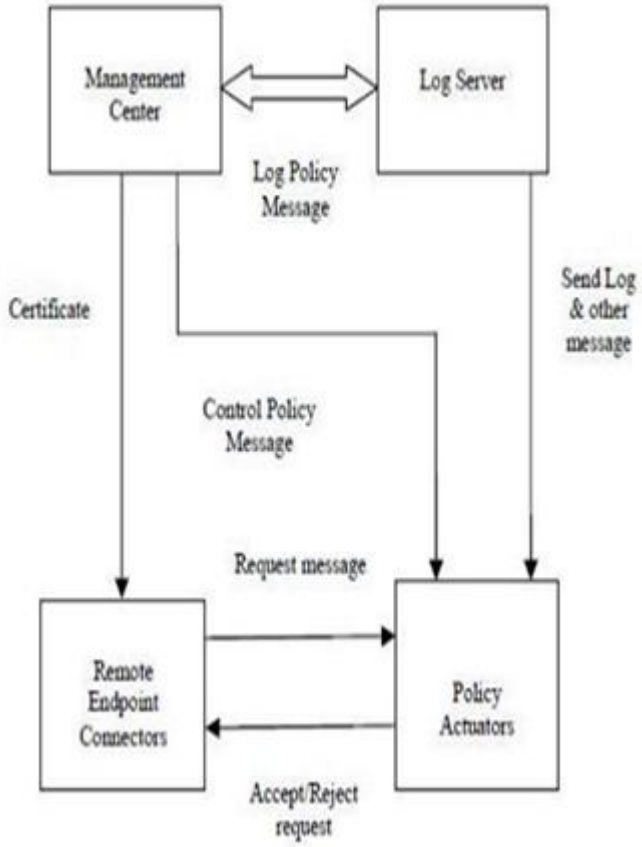

Figure 2 Distributed firewall architecture

3.4 Working with distributed firewalls

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 from 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. (Hiral B.Patel. et.al,2011)

IV. DATA SECURITY

4.1 Requirements of data security

The requirements of data security have undergone three major changes in the last decades.

1st major change: The first major change was the introduction of the computer. The need for protecting files and information became evident. Collection of tools designed to protect data and to avoid hacker attacks has the generic name "computer security".

2nd major change: The second major change was the introduction of distributed systems, networks and communication facilities for data communication. Data security Measures are needed to protect data during transmission.

3rd major change: The third change is the current, rapid development of wireless networks and mobile

4.1.1 IP Spoofing or IP Masquerading.

IP masquerading, means being an IP imposter. The server that is attacking our network server pretends to be someone else (with a different IP) and as a result is able to gain unlawful access to the server being attacked. This network data security threat is possible because of the inherent poor authentication in the IP protocol.

4.1.2 Physical access to servers in data centers

It is amazing that we get so involved in guarding against internet based network data security threats that we do not realize that physical unauthorized access to our data center servers is still the largest threat to internet network and data security. Good data centers have network data security protection in the form of fingerprint based authentication and verification of credentials of all operations personnel visiting the data center.(Badnera-Amravati,et.al,2013)**.**

V. NETWORK SECURITY AND BEST PRACTICES

5.1 Best practices

Network Data Security Practices are enumerated below:

Planning for an Optimum Network Data Security.

It is important to understand the concept of an optimum data security strategy to a user. There is really no perfect network data security strategy and security breaches will occur unless we work on a standalone PC. So, the network data security alternative is to provide a balance between access to servers and restricted access through network data security practices. (Mamta Joshi et.al, 2014)

Having a Well Thought Out Network Data Security Policy.

Everyone has a network data security policy. However, it is usually a piece of junk in an Attractive binder. That's the whole problem with a network data security policy. Consultants do make the comprehensive network data security policy but what is needed for a network data security policy is

to disseminate data security information handouts to all employees and contractors and to carry out a proper network data security audits.

5.2 Updating All Software's with Latest Patches.

The most frequent network data security attacks exploit the vulnerabilities of packaged software such as the operation system, the database or even specialized packages such as CRM or ERP packages. A typical solution to this network data security problem is to update our database software (example: Oracle) or operating system software (example Solaris) with the latest patches or upgrades.

5.3 Network Data Security Firewalls.

Get an industry standard network data security firewall and safeguard our network from unwarranted intrusions. Also, do carry out periodic audits of our network data security firewall rules so that our network data security is not compromised.

5.4 Policy enforcement

Policy enforcement is especially useful if the peer host is identified by a certificate. If so, the local host has a much stronger assurance of its identity than in a traditional firewall. In the latter case, all hosts on the inside are in some sense equal. If any such machines are subverted, they can launch attacks on hosts that they would not normally talk to, possibly by impersonating trusted hosts for protocols such as rlogin. With a distributed firewall, though, such spoofing is not possible; each host's identity is cryptographically assured.
Distributed firewalls

- Allow the network security policy to remain the control of the system administrators.
- Insiders may no longer be unconditionally treated as "trusted".
- Does not completely eliminate the need for traditional firewalls.
- More research is needed in this area to determine robustness, efficiency, and scalability.

5.5 Administrators

Policy is enforced by each individual host that participates in a distributed firewall. The security administrator who is no longer necessarily the "local" administrator, since we are no longer constrained by topology which defines the security policy in terms of host identifiers. The resulting policy (probably, though not necessarily, compiled to some convenient internal format) is then shipped out, much like any other change. This policy file is consulted before processing incoming or outgoing messages to verify their compliance. It is most natural to think of this happening at the network or transport layers but policies and enforcement can equally well apply to the application layer. (Mamta Joshi et.al, 2014)

VI. CONCLUSION AND FUTURE WORK

6.1 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.

Data Security along with a fast technological change is a demanding field. This overview shows that Data Security in itself must be seen as a whole. The adopted network security policy forms the basis. A proper choice of systems, protocols, standards and techniques gives the guidelines for a more secure networking.

6.2 Future Work

- High quality administration tools NEED to exist for distributed firewalls to be accepted.
- Allow per-packet scanning as opposed to per-connection scanning.
- Need for policy updating.

REFERENCES

[1] Pritish A. Tijare, Suraj J. Warade and Swapnil. N. Sawalkar "Data security in local network using distributed firewalls" [National Conference on Emerging Trends in Computer Technology (NCETCT-2014)]
[2] Jayshri V.Gaud and Mahip M.Bartere "Data security based on LAN using distributed firewalls" [International Journal of Computer Science and Mobile Computing. March 2014]
[3] Sneha Sahare, Mamta Joshi and Manish Gehlot "A survey paper data security in local networks using distributed

firewalls" [International Journal on Computer Science and Engineering (India); 09 Sep 2012]

[4] Hiral B.Patel, Ravi S. & Jayesh A.P. "Approach of data security in local network using distributed firewalls" [International Journal of P2P Network Trends and Technology- Volume1Issue3- 2011]

[5] *Prof.V.M.Deshmukh* and *Rajendra H.Rathod* "Roll of distributed firewalls in local network for data Security"Badnera-Amravati, India [International Journal of Computer Science and Applications Vol. 6, No.2, Apr 2013].

[6] Suraj J. Warade, Pritish A.Tijare and Swapnil. N. Sawalkar "A Review Data Security in Local Network using Distributed Firewall" [National Conference on Emerging Trends in Computer Technology - 2014]