DATA SECURITY IN LAN USING DISTRIBUTED FIREWALL

Dr.T.Pandikumar[1], Mekonnen Gidey[2]

[1]Associate Professor, Department of Computer & IT, Defence University, Ethiopia
[2]M.Tech, Department of Computer & IT, Defence University, Ethiopia

---***---

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***

1. INTRODUCTION

1.1 Back ground

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.

Traditional firewalls (Conventional 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 which often called perimeter firewalls. They divide the network into two parts; trusted on one side and un-trusted on the other side. For this reason they depend heavily on the topology of the network. Moreover, firewalls are a mechanism for policy control and permit a site administrator to set a policy on external access. Just as file permissions enforces an internal security policy and can enforces an external security policy.

1.2 Statements of the problem

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of services of a computer network and network-accessible resources. This network security can be achieved by firewalls. Those firewalls may be traditional or distributed firewalls. But 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. Some of the problems are:

- Reliance on the topology of the network.
- Do not protect networks from the internal attacks.
- Unable to handle some protocols like FTP.
- Have single entry point and the failure of these results into problems.
- Causes to network bottlenecks.
- Unauthorized entry points can bypass the network security

The Solution to this growing problem will never be found by simply improving the security technology of traditional firewall products.

1.3 Objectives of the Research Papers

The objective of this paper is to brief the solution to the problems of conventional firewalls. 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.

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.

1.4 Significance of these research works

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.

This document is template. We ask that authors follow some simple guidelines. In essence, we ask you to make your paper look exactly like this document. The easiest way to do this is simply to download the template, and replace (copy-paste) the content with your own material. Number the reference items consecutively in square brackets (e.g. [1]). However the authors name can be used along with the reference number in the running text. The order of reference in the running text should match with the list of references at the end of the paper.

2. CONVENTIONAL 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.

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 (Assumes inside users are “trusted”).
- Firewalls can become a bottleneck
- Multiple entry points make firewalls hard to manage
- Unable to handle protocols like FTP and Real-Audio.
- Single 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.

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.

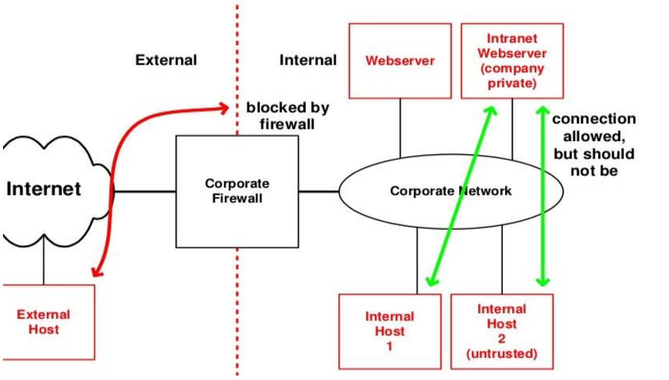


Figure 1 Standard firewall example, connection to intranet

3. 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.

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.

3.4 Architecture of distributed firewall

While the security policies are deployed in a decentralized way their management is not allowing system administrators to set policies from a central host and therefore still fulfill the requirements of efficient system and network administration. The whole distributed firewall system consists of four main parts:

1. **The management center**: The management center is responsible for the management of all endpoints in the network, security policy constitution and distribution, log file receiving from the host and analysis, intrusion detection and certain measure adoption.
2. **Policy actuator**: Policy actuator is installed in each host or gateway to receive the security policy issued by the management center, and to explain and implement the policy. It interprets and runs the security policy program. It is the real program to protect the endpoint host, and it is mainly to realize the function of the traditional firewall. Additionally, it is also to achieve the functions of communicating with the management control center and establishing communication link request for the remote endpoint.
3. **Remote endpoint connectors**: The remote endpoint connectors are the programs specifically designed for the remote endpoint host, to prove their identity to Maintaining the Integrity of the Specifications.
4. **Log server**: The log server is responsible for the collection of the various events occurred in the whole network, such as protocol rule log, user login event logs, user Internet access logs, for audit analysis.

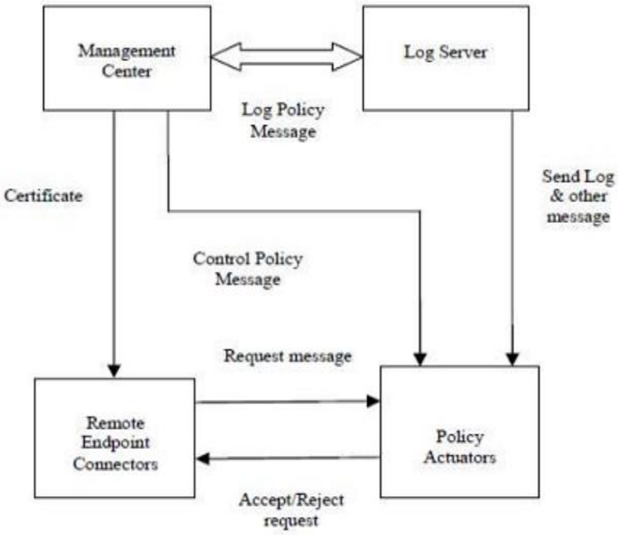


Figure 2 Distributed firewall architecture

3.5 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. 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.

3.6 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 or deny all other accesses.

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

3.7 Pull technique

The host 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. 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.

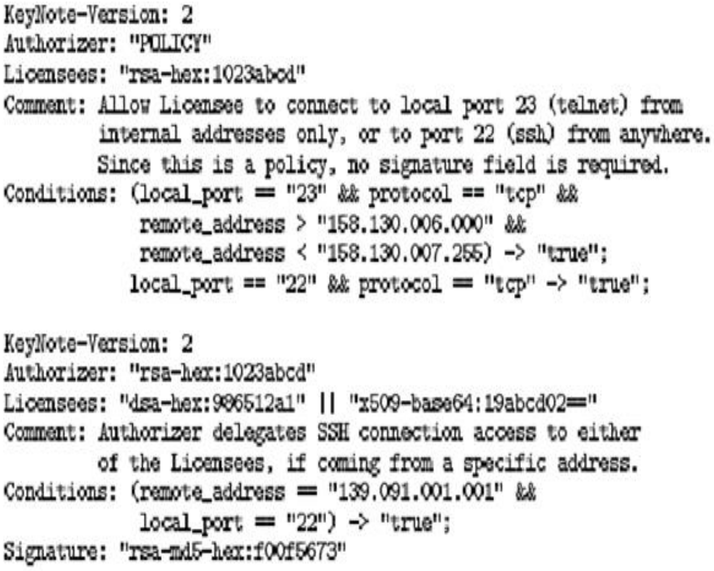
3.8 Push technique

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.

3.9 Distributed Firewall Implementation

3.9.1 Language: used to express policies and resolving requests (Keynote systems). Using keynote; IPSec allows control of mixed level policies where authentication mechanism is applied through public key cryptography.

3.9.2 Keynote system is a language to describe security policies (RFC 2704), all field names are case-insensitive and Blank lines are not permitted within an assertion. Policies and Credentials have same basic syntax, are "delegated" and MUST be signed



```
KeyNote-Version: 2
Authorizer: "POLICY"
Licensees: "rsa-hex:1023abcd"
Comment: Allow Licensee to connect to local port 23 (telnet) from
         internal addresses only, or to port 22 (ssh) from anywhere.
         Since this is a policy, no signature field is required.
Conditions: (local_port == "23" && protocol == "tcp" &&
             remote_address > "158.130.006.000" &&
             remote_address < "158.130.007.255) -> "true";
            local_port == "22" && protocol == "tcp" -> "true";

KeyNote-Version: 2
Authorizer: "rsa-hex:1023abcd"
Licensees: "dsa-hex:986512a1" || "x509-base64:19abcd02=="
Comment: Authorizer delegates SSH connection access to either
         of the Licensees, if coming from a specific address.
Conditions: (remote_address == "139.091.001.001" &&
             local_port == "22") -> "true";
Signature: "rsa-md5-hex:f00f5673"
```

Figure 3 keynote example

4. 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

communications. Data security is therefore of high priority today.

4.1 Data Security Threats

Security of Data is of much concern. Security measures taken are almost identical in the wired and wireless world. This implies specialized physical and data link protocols. Any network is subjected to substantial security risks and issues, Like threats to the physical security, eavesdropping and attacks from within the network's user community. Unauthorized Access can be of any means by which an unauthorized party is allowed access to network resources. Main Data Security Threats are:-

4.1.1 Denial of Service (DOS)

This network data security threat makes use of the simple fact that all servers have only a limited capacity to handle server requests. By making more requests to a network server than it can handle, this Network data security threat brings down the server. Denial of service has been used in the past to cause downtime of leading e-commerce firms, since it is an Easy network security threat to launch.

4.1.2 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.

4.1.3 Session Hijacking

Session hijacking implies taking control of a user's session resulting in a very serious data security breach. For example, a user may be accessing some mission critical data or making an internet purchase. At that time, a session hijacker takes control of the user session, thereby getting access to the sensitive session data. The user is led to believe that he has been logged out and he logs back in. Session hijacking is an incredibly dangerous network data security threat wherein the attacker could compromise sensitive user data such as passwords or even credit card information.

4.1.4 Physical access to servers in data centres

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.

5. NETWORK DATA SECURITY 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.

- **Data Centre Physical Security.**

A typical good network data security practice is to outsource the hosting of corporate servers to a data center that can focus on providing great network data security, data center disaster recovery and tough physical data center security. This implies posting a lot of burly security men at the data center, while simultaneously using advanced security gadgets to prevent direct access to servers by unauthorized personnel.

- **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 Network Data Securities Backups and Safeguarding

Use new network backup strategies such as remote data backups and data replication to take backups regularly, even when our systems are live. Also, safeguard our backups, as careless backup handling could be our biggest network internet data security threat.

5.5 Administrators

In a typical organizational environment, individuals are not necessarily the Administrators of the computers they use. Instead, to simplify system administration and to permit some level of central control, a system management package is used to administer individual machines. Patches can be installed, distribute new software etc. Same mechanisms are used in any event to control a distributed firewall. 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.

5.6 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. This is most easily understood by contrasting it to traditional packet filters. Consider the problem of electronic mail, because of a long-standing history of security problems in mailers, most sites with firewalls let only a few designated hosts receive mail from the outside. They in turn will relay the mail to internal mail servers. Traditional firewalls could express this by a rule that permitted SMTP (port 25) connections to the internal mail gateways; access to other internal hosts would be blocked. On the inside of the firewall, though, access to port 25 is unrestricted. With a distributed firewall, all machines have some rule concerning port 25. The mail gateway permits anyone to connect to that port; other internal machines, however, permit contact only from the mail gateway, as identified by its certificate.

6. 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. The security levels of current networks must be constantly enhanced to meet the growing security threats. Wired and wireless networks use in principal the same type of basic security methods. This means that security measures taken to ensure the integrity and security of data in the wired local area network environment are also applicable to wireless LANs. Information systems are strongly affected by secure wireless technology. In the near future we will see a rapid growth of wireless technology, devices and equipment. Security aspects will enhance this change and the effect on information systems will be significant.

Distributed Firewall gives complete protection to the network. It protects all the clients of the networks from the internal and external attacks. The distributed firewall system can allow or deny the traffic meant for a particular system based on the policy it has to follow. Remote end-user machines can be secured so they can't be used as entry points into the enterprise network. 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. Because the firewall is distributed across an entire network or server farm it offers unlimited scalability. The processing load is further distributed as the network grows, so performance remains high.

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.

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.

7 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]

[7] Sotiris Ioannidis**,** Angelos D. Keromytis, Steve M. Bellovin and Jonathan M. Smith **[**"Implementing a Distributed Firewall" 2013**]**