Available at: www.researchpublications.org

Roll of Distributed Firewalls in Local Network for Data Security

***RAJENDRA H. RATHOD*[1], M.E. (Pursuing), Computer Science and Engineering
Prof.RamMeghe Institute of Technology & Research, Badnera-Amravati : 444701
rh_rathod@yahoo.com

***Prof.V.M.DESHMUKH,*[2]**

Prof.RamMeghe Institute of Technology & Research, Badnera-Amravati : 444701

ABSTRACT:*Network Security is needed to prevent hacking of data and to provide authenticated data transfer. Network Security can be achieved by Firewall. Firewall is a hardware or software device designed to permit or deny network transmissions based upon a set of rules and regulation. It is frequently used to protect networks from unauthorized access.A firewall is typically placed at the edge of a system and acts as a filter for unauthorized traffic. But conventional firewalls rely on the notions of restricted topology and controlled entry points to function. Restricting the network topology, results in difficulty in filtering of certain protocols, End-to-End encryption problems etc.Sodistributed firewalls are used which allow enforcement of security policies on a network without restricting its topology on an inside or outside point of view. 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. They provide unlimited scalability and also they overcome the single point of failure problem presented by the perimeter firewall.*

This paper is a literature review 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.

1. INTRODUCTION

In today's world, most businesses, regardless of size, believe that access to the Internet is imperative if they are going to compete effectively. Even though the benefits of connecting to the Internet are considerable, so are the risks. 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. A number of confidential transactions occur every second and today computers are used mostly for transmission rather than processing of data. We need some approach to 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 **[2]**.It is a Network Security needed to prevent hacking of data and to provide authenticated data transfer. This Network Security can be achieved by Firewalls.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**[1]**. 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, as in Figure-1. For this reason they depend heavily on the topology of the network.In general, firewalls can be categorized under one of two general types:

- Desktop or personal firewalls
- Network firewalls

Within the network firewall type, there are primary classifications of devices, including the following:

- Packet-filtering firewalls (stateful and nonstateful)
- Circuit-level gateways
- Application-level gateways**[2]**, **[19]**

2. LITERATURE REVIEW

The various papers over the distributed firewall was searched as follows and literature review is given as:

1994: Bellovin, S.M. and W.R. Cheswick, "*Firewalls and Internet Security: Repelling the Wily Hacker*", Addison-Wesley. In this paper he suggested that the distributed firewall design is based on the idea ofenforcing the policy rules at the endpoints rather than a single entry point to network.

1994: William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, first edition.

1999: Steven M. Bellovin, "*Distributed Firewalls*", November 1999 issue of; login: pp. 37-39. Suggested advantages of distributed firewalls over standard firewall

1999: William Stalling, "*Cryptography and Network Security Principles and Practices*", ISBN-978-81-775-8774-6, PEARSON

2000: 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.

2001: Robert Stepanek, Distributed Firewalls In Article In T-110.501Seminar on Network security 2001

2003: Cheswick, W.R., Bellovin, S.M., Rubin, A.D.: *Firewalls and Internet Security*, Repelling the Wily Hacker, 2nd edn. AddisonWesley.

2011: HiralB.Patel, 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

2012: SnehaSahare, Mamta Joshi, ManishGehlot "*A Survey paper: Data Security in Local Networks Using Distributed Firewall*" ISSN : 0975-3397 Vol. 4 No. 09 Sep 2012, 1617

3. STANDARD FIREWALL

This paper is a literature survey of standard firewall and distributed firewall. A standard firewall has certain policies to protect the data from outsiders. But not all the data or information can be protected internally from insiders of the network. Some problems with standard firewall 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 sourceaddresses).
6) Unable to log all of the network's activity and unable to dynamically open and close their networking ports.**[3]**

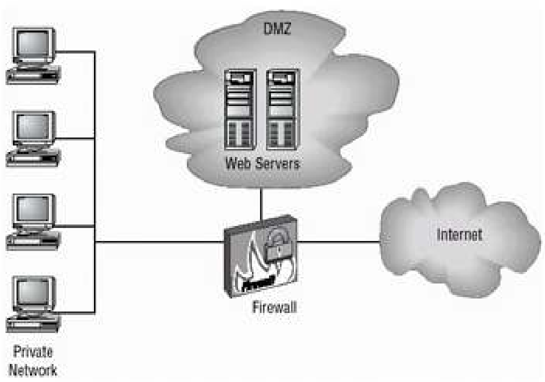


Figure-1: A conventional firewall

To solve these problems of the traditional firewall, the evolution of the distributed firewall comes into picture.They provide virtually unlimited scalability. In addition, theyovercome the single point-of-failure problempresented by the perimeter 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 called inside attack.**[2], [13]**

4. A DISTRIBUTED FIREWALL DESIGN

Distributed firewallsare 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 as given in the figure-2 and figure-3.Usually deployed behind the traditional firewall, they provide a second layer of protection. Distributed firewalls secure thenetwork 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.**[8]**

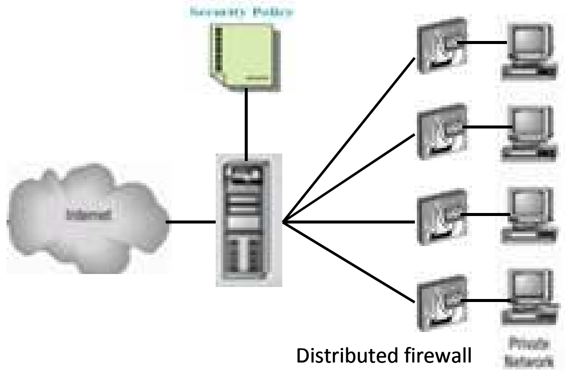


Figure-2 : distributed firewall

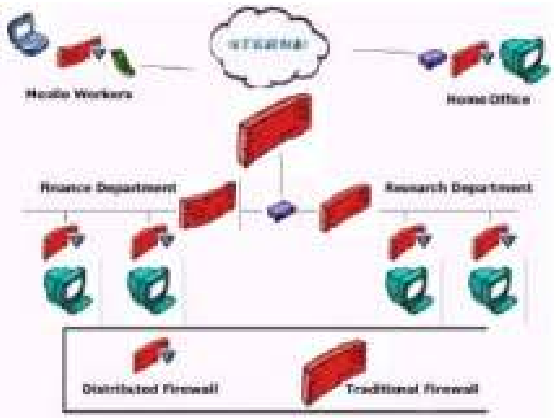


Figure-3 : Distributed firewall Architecture

The distributed firewall design is based on the idea ofenforcing 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 theadvantages of firewalls while resolving the disadvantages.**[14]**
They guard the individual machine in the same way that the perimeter firewall guards the overall network.

4. COMPONENTS OF A DISTRIBUTED FIREWALL

There are three components of distributed firewall.
i. Policy language
ii. Policy distribution scheme
iii. Certificate
Policy language defines which inbound and outbound connections are allowed or rejected. It is equivalent to packet filtering rules. Policy language should also support credential for authentication purpose **[8].**
Distributed firewall use cryptographic certificates as identifier since these are independent of topology. Certificate enables making decisions without knowledge of the physical location of the host.
Policy distribution scheme is used to enable policy control from central point from central point.

5. ADVANTAGES OF DISTRIBUTEDFIREWALLS

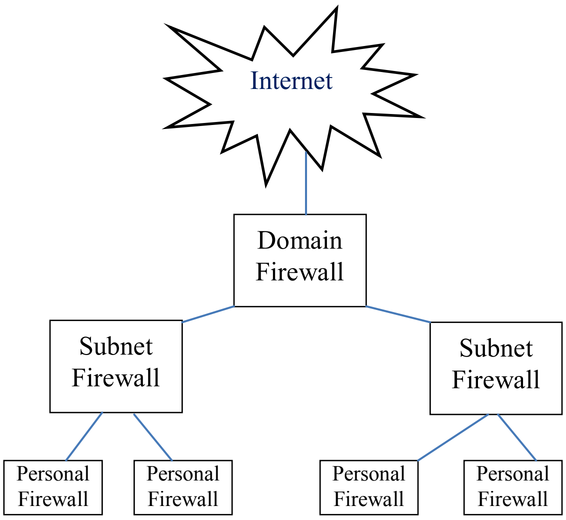
- Topological independence is one of the main advantages of distributed firewalls. Since network security no longer depends on network topology, it provides more flexibility in defining the security perimeter.**[1]**
- Network security is no more dependent on the single firewall so that problems like performance bottleneck and traffic congestion are resolved.**[8], [12]**
- 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, whichis the end host in general.**[2], [9], [12]**
- 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.**[9]**
- 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. **[9], [12]**
- End-to-end encryption is possible without affecting the network security, significantly improves the security of the distributed firewall.**[5]**

6. DISADVANTAGESOF DISTRIBUTEDFIREWALLS

- If firewall command center is compromised, due to attack or mistake by the administrator, this situation is high risky for security of the entire network
- Intrusion detection systems are less effective with distributed firewalls because complete network traffic is not on the single point.
- 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. **[10], [11],[12], [14]**

7. DISTRIBUTED FIREWALL: ADMINISTRATION ARCHITECTURE

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 tothe 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 numberof 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 haveto 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 viathe subnet firewall. **[22]**

7. CONCLUSION

This paper try toprovide the solution over computer crime whenever user can transfer sensitive and important data orinformation using firewalls and distributed firewalls which provides the security during the data transmission. Theyprovide the legal infrastructure for internet access. Firewallsprovide the facility like only authentic user can access thecomputer or internet for his personal use**[20]**. Distributed firewall can solve some known and thoroughly discussed problems which arisewith the use of conventional firewalls residing at the networks perimeter. It's independenceon topological constraints reflect the change in enterprise and other organizations networkorganization more accurately but demand fundamental changes in the network end-pointsoperating systems.

In this paper we have tried to explain or provethe internet problems and solution of that problem with thehelp of distributed firewalls. It is also called filtering process.Network security policy specification remains under the control of the network administrator in distributed firewall network system.Since enforcement occurs at the endpoints, various shortcomings of traditional firewalls are overcome:

- Security is no longer dependent on restricting the network topology. This allows considerable flexibility in defining the "security perimeter," which can easily be extended to safely include remote hosts and networks.
- Since we no longer solely depend on a single firewall for protection, we eliminate a performance bottleneck. Alternately, the burden placed on the traditional firewall is lessened significantly, since it delegates a lot of the filtering to the end hosts.
- Filtering of certain protocols (e.g., FTP) which was difficult when done on a traditional firewall, becomes significantly easier, since all the relevant information is present at the decision point, i.e., the end host.
- The number of outside connections the protected network is no longer a cause for administration nightmares. Adding or removing links has no impact on the security of the network. "Backdoor" connections set up by users, either intentionally or inadvertently, also do not create windows of vulnerability.
- End-to-end encryption is made possible without sacrificing security, as was the case with traditional firewalls. In fact, end-to-end encryption greatly improves the security of the distributed firewall.
- Application-specific policies may be made available to end applications over the same distribution channel.
- Filtering (and other policy) rules are distributed and established on an as-needed basis; that is, only the hosts that actually need to communicate need to determine what the relevant policy with regard to each other is. This significantly eases the task of policy updating, and does not require each host/firewall to maintain the complete set of policies, which may be very large for large networks. Furthermore, policies and their distribution scales much better with respect to the network size and user base than a more tightly-coupled and synchronized approach would.

On the other hand, distributed firewall architecture requires high quality administration tools. The introduction of a distributed firewall infrastructure in a network does not completely eliminate the need for a traditional firewall.

- It is easier to counter infrastructure attacks that operate at a level lower than the distributed firewall.
- Denial-of-service attack mitigation is more effective at the network ingress points
- Intrusion detection systems are more effective when located at a traditional firewall, where complete traffic information is available.
- The traditional firewall may protect end hosts that do not (or cannot) support the distributed firewall mechanisms. Integration with the policy specification and distribution mechanisms is especially important here, to avoid duplicated filters and windows of vulnerability.
- Finally, a traditional firewall may simply act as a fail-safe security mechanism.

Fully distributed firewall architecture is very similar to a network with a large number of internal firewalls.

ACKNOWLEDGMENT

First and foremost I want to thank my GuideSmt.V.M.Deshmukhmadom. With great pleasure and gratefulness, I extend my deep sense of gratitude to Prof.Dr.G.R.BamnoteSir, HOD, ComputerEngg. Deptt.for giving me an opportunity to accomplish my paper and to increasemy knowledge.AlsoI want to thank to Dr.Gupta sir to help me time to time. Lastly I wish to thank each and every person involved in making my dissertation successful. Thank You.

REFERENCES

[1] http://www.seminarprojects.com/*Thread-data-security-in-localnetwork-using-distributed-Firewalls*

[2] http://en.wikipedia.org

[3] HiralB.Patel, 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.

[5] AtulKahate, "*Cryptography and Network Security*", ISBN-13: 978-0-07-064823-4, ISBN-10: 0-07-064823-9, McGraw Hill Higher Education.

[7] Robert Stepanek, Distributed Firewalls In Article In T-110.501Seminar on Network security 2001

[8] 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.

[9]Behrouz A. Forouzan, DebdeepMukhopadhyay, "*Cryptography and Network Security*", ISBN-13: 978-0- 07-070208-0, ISBN-10: 0-07-070208-X, McGrawHill Higher Education.

[10] Steven M. Bellovin, "*Distributed Firewalls*", November 1999 issue of; login: pp. 37-39.

[11] Daniel Wan, "*Distributed Firewall*", GSEC Practical Assignment Version 1.2c.

[12] William Stalling, "*Cryptography and Network Security Principles and Practices*", ISBN-978-81-775-8774-6, PEARSON

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

[14] Bellovin, S.M. and W.R. Cheswick, "*Firewalls and Internet Security: Repelling the Wily Hacker*", Addison-Wesley, 1994.

[15] SnehaSahare, Mamta Joshi, ManishGehlot "*A Survey paper: Data Security in Local Networks Using Distributed Firewall*" ISSN : 0975-3397 Vol. 4 No. 09 Sep 2012, 1617

[16] Scuba, C.L., Spafford, E.H.: Reference model for firewall technology, Source. In: Annual Computer Security Applications Conference, pp. 133–145 (1997)

[17] William R. Cheswick and Steven M. Bellovin.*Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, first edition, 1994

[18] Cheswick, W.R., Bellovin, S.M., Rubin, A.D.: *Firewalls and Internet Security*, Repelling the Wily Hacker, 2nd edn. AddisonWesley (2003)

[19] Behrouz A. Forouzan, DebdeepMukhopadhyay, "*Cryptography and Network Security*", ISBN-13: 978-0- 07-070208-0, ISBN-10: 0-07-070208-X, McGraw Hill Higher Education.

[20] Mark, Stuart."*Distributin g firewall tasks*" 23 April 2001

[21]Fogei, Avi. "Distributed firewalls provide options for security topology" July 2000

[22]Yunus ERDOĞAN "Development of a Distributed Firewall Administration tool November 2008