INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DATA SECURITY IN LOCAL NETWORK USING DISTRIBUTED FIREWALL

BHAGYASHREE S. THAKUR[1], PRANJALI P. DESHMUKH[2]

1. M. E. Scholar, department of CSE, P. R. Pote (Patil) College of Engineering, Amravati, India.
2. HOD, P. R. Pote (Patil) College of Engineering, Amravati, India

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Network Security is needed to prevent hacking of data and to provide authenticated data transfer. Computer and Network security are the means of prevention and detection of unauthorized actions by users of computer system. The unauthorized action can be defined by the security policies which defines the security rules of a system. In most of the systems, the network security is 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 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. 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 literature review paper,dealing with the general concepts such as distributed firewalls, its requirements and implications and introduce, its suitability to common threats on the Internet. A distributed firewall gives complete security to the network.

Keywords: Network Security, Policy Language, Certificate, Distributed Firewall, pull technique, push technique

PAPER-QR CODE

Corresponding Author: MS. BHAGYASHREE S. THAKUR

Access Online On:

www.ijpret.com

How to Cite This Article:

Bhagyashree Thakur, IJPRET, 2014; Volume 2 (9): 825-834

INTRODUCTION

Now a day's no one would think a life without computers and the Internet, they both are become inseparable. 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 data.

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. This Network Security can be achieved by Firewalls. conventional firewall 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 problem and few more problems lead to the evolution of Distributed firewalls.

Distributed firewall is a mechanism to enforce a network domain security 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.

Distributed firewall 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.

Distributed firewall are host-resident security software application that protect the enterprise network 's server and end users machine against unwanted intrusion.

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 of enforcing 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: Hiral B.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, Manish Gehlot “A Survey paper: Data Security in Local Networks Using Distributed Firewall” ISSN :0975-3397 Vol. 4 No. 09 Sep 2012, 1617 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

Real Audio.

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.

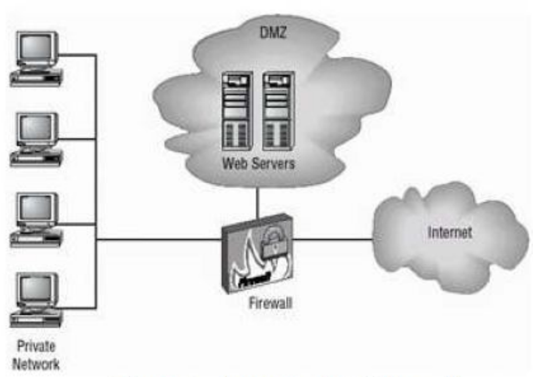


Figure-1: A conventional firewall

To solve these problems of the firewall the evolution of the distributed firewall comes into scenario. 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. 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. Distribute firewall solves these problems and protecting critical network end points where hackers want to penetrate. It filters the traffic from both the internal network and Internet because most destructive and costly hacking attacks still originate within organization.

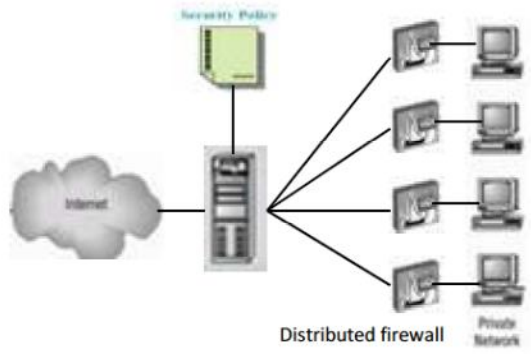


Figure-2 : distributed firewall

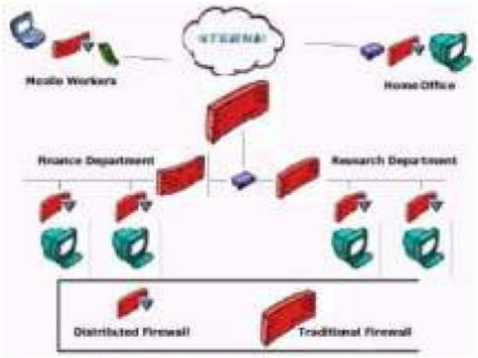


Figure-3 : Distributed firewall Architecture

In this architecture, the security policy is still defined centrally ,but the enforcement of the policy takes place at each endpoint (hosts, routers,etc). The centralized policy defines what connectivity is permitted or denied. Then this policy is distributed to all endpoints, where it is enforced. There are three components of distributed firewall.

i. Policy language

ii Policy distribution scheme

iii. Certificate (an authentication and encryption mechanism, such as IPSec.)

The *security policy language* describes what connections are permitted or prohibited. It should support credentials and different types of applications. After policy is compiled, it is shipped to endpoints.

The *policy distribution scheme* should guarantee the integrity of the policy during transfer. This policy is consulted before processing the incoming or outgoing messages. 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, or it may even be provided to the users in the form of credentials that they use when they try to communicate with the hosts.

Distributed firewalls use IP addresses for host identification. But a secure mechanism is more desirable. It is preferred to use certificate to identify hosts. IPSec provides cryptographic *certificates.* These certificates can be very reliable and unique identifiers. Unlike IP address, which can be easily spoofed, the digital certificate is much more secure and the ownership of a certificate is not easily forged. Furthermore, they are also independent of topology. Policy is distributed according to these certificates. If a machine is granted certain privileges based on its certificate, those privileges can be applied regardless of where the machine is physically located. In this case, all machines have the some rules. They will apply the rules to the traffic.Since they have better knowledge of the connection (such as the state and the encryption keys, etc), they will make better judgment according to the policy. With a distributed firewall, the spoofing is not possible either, because each host's identity is cryptographically assured.

3. Advantages Of Distributed Firewalls

- 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.

- Network security is no more dependent on the single firewall so that problems like performance bottleneck and traffic congestion are resolved.

- 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.

- 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.

- End-to-end encryption is possible without affecting the network security, significantly improves the security of the distributed firewall.

4.Disadvantages Of Distributed Firewalls

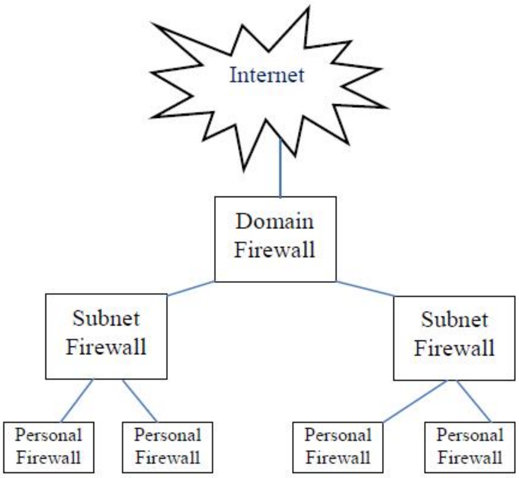
- If firewall command center is compromised, due to attack or mistake by the administrator, this situation is high risky for security of the entire network.

- 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.

- Intrusion detection is harder to achieve on distributed firewalls. Modern firewalls can detect the attempted intrusions. In a distributed firewall, it is not a problem for a host to detect the intrusions, but the collection of data is more problematic, especially at times of poor connectivity to the central site, or when the either site (host or central site) is under attacks such as DoS.

5. 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 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 viat he subnet firewall.

7. CONCLUSION

This paper try to provide the solution over computer crime whenever user can transfer sensitive and important data or information using firewalls and distributed firewalls which provides the security during the data transmission. They provide the legal infrastructure for internet access. Firewalls provide the facility like only authentic user can access the computer or internet for his personal use. Distributed firewall can solve some known and thoroughly discussed problems which arise with the use of conventional firewalls residing at the networks perimeter. It's independence on topological constraints reflect the change in enterprise and other organizations network organization more accurately but demand fundamental changes in the network end points operating systems.

6. RESULT AND DISCUSSION

In this paper i have tried to explain or prove the internet problems and solution of that problem with the help 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.

7. ACKNOWLEDGMENT

First and foremost, I extend my deep sense of gratitude to my Guide Prof. P. P. Deshmukh madam. H. O. D. computer science and engg Dept. for giving me an opportunity to accomplish my paper and to increase my knowledge. I wish to thank each and every person involved in making my dissertation successful. Thank You.

8. 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. AtulKahate, “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, November 2000, Athens, Greece.

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

8. Steven M. Bellovin, "Distributed Firewalls", November 1999 issue of; login: pp. 37-39.

9. Daniel Wan, "Distributed Firewall", GSEC Practical Assignment Version 1.2c.

10. William Stalling, "Cryptography and Network Security Principles and Practices", ISBN-978-81-775-8774-6, PEARSON

11. Anand Kumar "Data security in local networks using distributed firewalls", Cochin University of science and technology, August-2008

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

13. 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

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

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

16. 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.

17. Mark, Stuart."Distributin g firewall tasks" 23 April 2001

18. Fogei, Avi. "Distributed firewalls provide options for security topology" July 2000

19. Yunus ERDOĞAN "Development of a Distributed Firewall Administration tool November 2008

20. Daniel Wan "Distributed Firewall"(GSEC Practical Assignment Version 1.2c).

21. RAJENDRA H. RATHOD" Roll of Distributed Firewalls in Local Network for Data Security" ISSN: 0974-1011 (Open Access) Apr 2013.