ISSN (e): 2250 – 3005 || Volume, 08 || Issue, 03|| March – 2018 ||
International Journal of Computational Engineering Research (IJCER)

Data Security in Local Area Network using Policy Distribution

Rajesh Kumar Pati[1],, Satyabrata Dash[2],Pratyush Ranjan Mohapatra[3]
[1,3]*Associate Professor, Department of Computer Science&Engineering, Gandhi Institute For Technology (GIFT), Bhubaneswar*
[2] *Assistant Professor, Department of Computer Science &Engineering, Gandhi Engineering College, Bhubaneswar*

Abstract: *With tremendous increase in internet connection, the data security is important aspect for researchers and developers. The importance of network security increases as the use of internet increases for communication, data transfer. Thesecurity can be achieved by firewall. The conventional firewall is placed between the two network or entry point of one of the network. So, the data comingin the network is coming fromsinglesecureentry point and as the firewall is at the entry point of the network all inside the network are trusted. To remove the shortcomings of traditional firewalls, the concept of a "distributed firewall" has been proposed. In this scheme, security policy is still centrally defined, but enforcement is left up to the individualendpoints.*
Index Terms- *Distributed Firewall; Network Security; Pull Technique; Push Technique; Policy Distribution*

I. INTRODUCTION

All the necessary information in daily life is available on the internet. So, Internet Connectivity is no longer optionalfor anypersonororganizationAndnowcomputersaremostlyuse for transfer of data than the processing. So, Network Security is needed to provide authenticated data transfer for secure communication.Afirewallisadevicewhichdecidestopermit or deny the network transmission. Conventional firewalls are situatedattheentrypointofanetworkandhencethefailureof that single entry point causes to fall of network security[1].

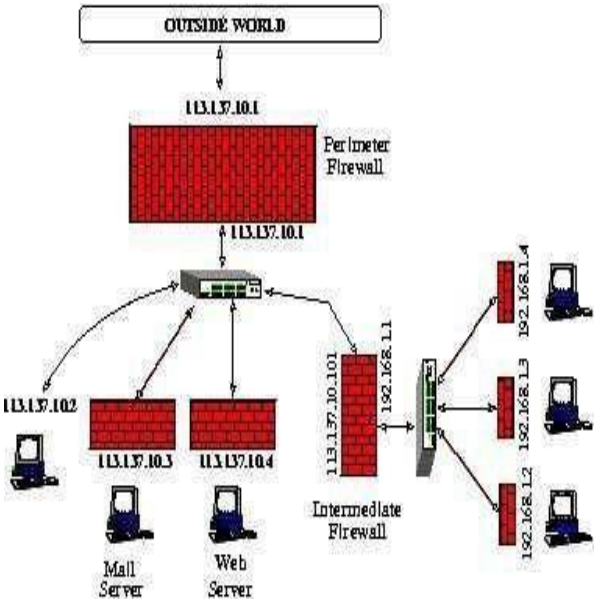
The Distributed firewall is centrally managed and distributed over the network with the connected systems i.e. with end points. In the distributed firewall the security policy is centrally defined and implemented at the end host. As distributed firewall implemented at the end host security no longer depends upon the single entry point. The Distributed firewall filters the data from internet as well as internal network. In the distributed firewall data on the protected side is not taken as trusted and hence the attacks which happens from inside are detected [2].

The problems with conventional firewalls which lead to implement Distributed Firewalls are as follows.

- Depends on the topology of the network[3].
- Do not protect networks from the internal attacks[3].
- Unable to handle some protocols like FTP and Real audio [3].
- Havesingleentrypointandthefailureoftheseresults into problems[3].
- Network bottleneck and congestion[3].
- Unauthorized entry points can bypass the network security[3].
- GENERALIZED DISTRIBUTEDFIREWALL

In Distributedfirewall,Theconventionalfirewallisnotonly placed at the entry point of one network or between the two networks. The roll of conventional firewall is distributed over a network. At each end host system have a firewall typically underacontrolofcentralizedsystemwhichdefinesthepolicies implemented at the end host. Because of distributed behavior thebottleneck,congestion,failureofsingleentrypointsarenot occurred.

Figure 1: Generalized Distributed Firewal



In the figure above a conventionalfirewallismaintainedat the network border, although the presence of a distributed firewall solution is being deployed to protect each network endpoint.

II. POLICIES OFDISTRIBUTED FIREWALL

Policy is one of the most often used terms in case of network security and in particular distributed firewall. A "security policy" defines the security criteria of a system. The security policy is defined for whom transmission is allowed or denies.Withtheimplementationofthedistributedfirewallsthe policy can be varies. It can be pulled to end host or pushed whenever necessary.

3.1. Pulltechnique

The end host checks by sending some ping whether the central management server is up and active. It registers the central management server and requests for the policies which it should implement. In reply the central management server provides the security policies to the end host [4, 5].

3.2. Push technique

Whenever the policies at the central management system changes by the network administrator push technique is applied. The push technique always keep the end host updated with the security policies [4, 5].

III. COMPONENTS OFDISTRIBUTED FIREWALL

- A central management system for designing the policies.
- Policy distribution to transmit thesepolices.
- Host-end implementation of the designed policies in the clientend.

4.1. Central managementsystem

Central Management Servers main work is designing the policies. It is a component of distributed firewalls which makes it practical to secure organizational systems. It maximize network security by enabling policies which are centrally configured [5].

4.2. Policydistribution

The policy distribution scheme should guarantee the originalityofthepolicyduringtransfer.Thedistributionof the policy can be different and varies with the implementation.It can be either directly pushed to end systems, or pulled when required [5].

4.3. Host-end implementation

The policies from central management server should be implemented at the end host. The correct host end implementation is necessary for success of distributed firewall [5].

IV. LITRATUREREVIEW

A lot of work has been done over the previous years in the area of firewalls. It describes the host resident approach of firewall, similarly as we have discussed in this paper.

One of the first conversations of distributed firewalls was given by Bellovin, which described a distributed system of firewalls with a security policy, but the security policy is centrally managed [7].

TheNapoleonsystemdefinesalayeredgroup-basedaccess control scheme that is in some ways similar to the distributed firewall and it is mostly targeted to RMIenvironments[5].

Ehab Al-Shaer, HazemHamed, RaoufBoutaba, and Masum Hasan presented a set of algorithms and techniques to automatically discover rule anomalies in centralized and distributed firewalls [8].

Yunus Erdogan gives discussion about Development of a Distributed Firewall Administration tool [9].

Ongoing development and research in the field of firewall technology have shown a continuous addition of features and services to conventional firewall systems as well as applying the concept of distributed firewalls in new products.

V. ADVANTAGES OFDISTRIBUTED FIREWALL

(1) Does not depend on topology ofnetwork.
(2) BecauseofDistributedbehaviorProtectfrominternal threads.
(3) Able to handle protocol like FTP and Realaudio.
(4) May have multiple secure entrypoints.
(5) Do not occurs bottleneck and congestion because multiple secure entrypoints.

VI. DISADVANTAGES OFDISTRIBUTED FIREWALL

(1) If the Central Management System is compromised, due to attack or mistake by the administrator, this situation is very risky for security of the entire network.
(2) It is not so easy to implement an intrusion detection system in a distributed firewall environment [7,10].

VII. CONCLUSION

With the vast use of internet for data transfer the conventional firewall is not enough for providing secure authenticateddata.So,byusingdistributedfirewallconceptwe canachieve,

- Complete protection to thenetwork.
- Protection to the clients of the networks from the internal and externalattacks.
- Can allow or deny the traffic meant for a particular system based on the policy it has tofollow.
- Because the firewall is distributed across an entire network, the load of processing is further distributed as the network grows, so performance remainshigh.

REFERENCES

[1]. 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 2017, Athens, Greece.
[2]. Behrouz A. Forouzan, DebdeepMukhopadhyay, "Cryptography and Network Security", ISBN-13: 978-0- 07-070208-0, ISBN-10: 0-07-070208-X, McGrawHill HigherEducation.
[3]. RajendraH.Rathod,V.M.Deshmukh"RollofDistributedfirewall in local network for Data Security" International Journal Of Computer Science And Applications Vol. 6, No.2, April2013
[4]. 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.
[5]. en.wikipedia.org/wiki/Distributed_firewall.
[6]. Robert Stepanek, "Distributed Firewalls", rost@cc.hut.fi,T-110.501 Seminar on Network Security, HUT TML 2001.
[7]. Steven M. Bellovin, "Distributed Firewalls", November 1999 issue of; login: pp.37-39.
[8]. EhabAl-Shaer,HazemHamed,RaoufBoutaba,andMasumHasan "Conflict Classification and Analysis of Distributed Firewall Policies." IEEE Journal in selected areas in communication VOL. 23, NO. 10, October2005.
[9]. Yunus ERDOGAN " Development of a Distributed Firewall Administration tool " November2008.
[10]. Bellovin, S.M. and W.R. Cheswick,"Firewalls and Internet Security: Repelling the Wily Hacker",Addison-Wesley,1994.