Data Security in Local Network using Distributed Firewall: A Review

Suraj J. Warade
2 nd Sem M.E,Computer Engineering
Sipna C.O.E.T, Amaravati, India

Pritish A. Tijare
Dept. Computer Science and Engineering
Sipna C.O.E.T, Amaravati, India

Swapnil. N. Sawalkar
Dept. Computer Science and Engineering
Sipna C.O.E.T, Amaravati, India

ABSTRACT
With the vast internet connections, the network security gained the attention of researcher and developers. Network Security is important for providing the authenticated data transfer. Network security can be achieve by the firewall. The Conventional firewall acts like a filter which restricts the unauthorized traffic. Firewall is situated at the entry point of a network. In Conventional firewall everyone on the protected side is trusted. To remove the shortcomings of traditional firewalls, the concept of a "distributed firewall" has been proposed. In which security policy is still centrally defined, but implementation is at individual endpoints.

Index Terms
Network Security, Distributed Firewall.

1. INTRODUCTION
Internet Connectivity is no longer optional for a person or any organization. All the necessary information in daily life is available on the internet. And now computers are mostly use for transmission of data than the processing. So, Network Security is needed to provide authenticated data transfer and to prevent hacking of data.

A firewall is a device between two networks that filters the transmission between them according to the security policy used, i.e. a device which decides to permit or deny the network transmission. Traditional firewalls are situated at the entry point of a network and hence the failure of that single entry point causes to fall of network security [1]. The Distributed firewall no longer depends upon the single entry point.

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. The Distributed firewall filters the data traffic from internet as well as internal network. Because of the distributed nature the data on the protected side is not taken as trusted and hence the attacks which happens mostly from inside are detected and prevented[2].

2. ISSUES WITH CONVENTIONAL FIREWALLS

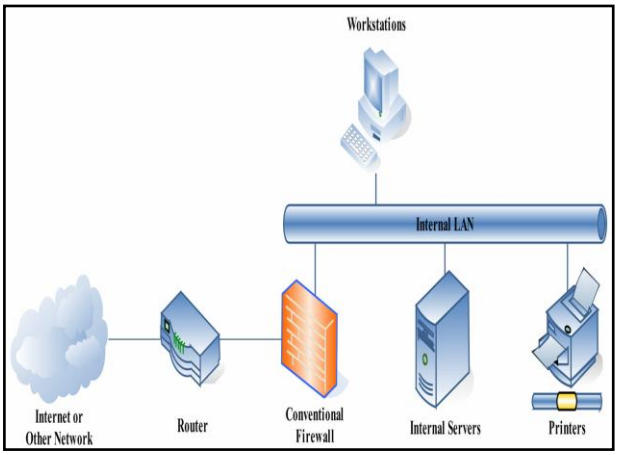

Figure : Conventional Firewall

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

- Reliance on the topology of the network [3].
- Do not protect networks from the internal attacks [3].
- Unable to handle some protocols like FTP [3].
- Has single entry point and the failure of this results into problems [3].
- Causes to network bottlenecks.
- Unauthorized entry points can bypass the network security.

3. DISTRIBUTED FIREWALLS
In Distributed Firewall systems, The conventional firewall is not only placed at the entry point of one network or between the two networks the role of conventional firewall is distributed among the all devices connected in the network under the control of centralized system which is also used to define the policy granted by the distributed firewall system which is going to apply at each end devices.

The conventional firewall is distributed over a network which solves the problem of single entry point failure i.e. if the network entry point firewall fails the host resident firewalls secure the network from intrusion.

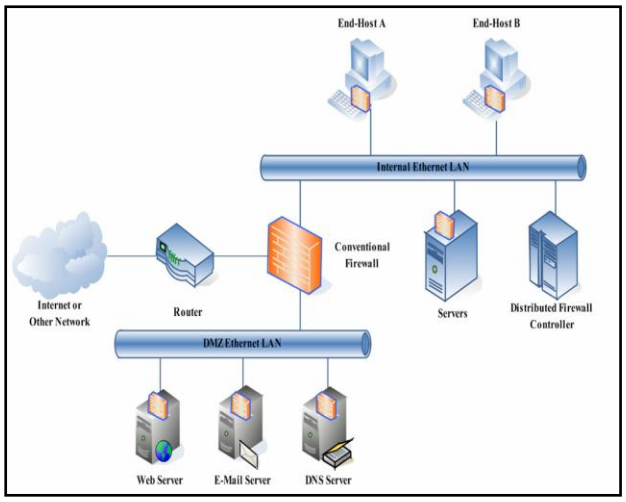

Figure: Generalized Distributed Firewall

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

4. POLICIES OF DISTIBUTED 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.

Simple example for a firewall is:

- Deny all connections to the web server.
- Allow all other access.

With the implementation of the distributed firewalls the policy can be varies. It can be pulled to end host or pushed whenever necessary.

4.1 Pull Technique

The end host checks whether the central management server is up and active by sending some ping, it registers the central management server and requests for the policies which it shoud implement. In reply the centreal management server i.e distributed firewall controller provides the host security policies [4], [5].

4.2 Push Technique

When policies are updated at the central management side by the network administrator the push technology is applied. The push technology is confirm that the end host always have updated policies [4], [5].

5. COMPONENTS OF DISTRIBUTED FIREWALL

- A central management system.
- Policy distribution.
- Host end implementation.

5.1 Central Management System

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

5.2 Policy Distribution

The policy distribution scheme should guarantee the reliability of the policy during transfer. With the implementation, distribution of the policy can be different and varies. It can be either directly pushed to end systems, or pulled when required [5].

5.3 Host-end Implementation

The security policy transmitted from the central management server has to be implemented by the end host [5].

6. RELATED WORK

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].

The Napoleon system defines a layered group-based access control scheme that is in some ways similar to the distributed firewall and it is mostly targeted to RMI environments[5].

Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba, 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 [6].

7. ADVANTAGES USING DISTRIBUTED FIREWALL

Sr. No.	Parameter	Conventional Firewall	Distributed Firewall
01	Topology	Depends upon topology of network	Does not depend on topology of network.
02	Internal Threads	Do not protect from internal threads	Protect from internal threads.
03	Handling protocol	Unable to handle protocols like FTP and Real Audio	Able to handle protocol like FTP and Real Audio
04	Entry points	Have only single secure entry point	May have multiple secure entry points
05	Bottleneck and Congestion	Occurs because of single secure entry points	Do not occurs because multiple secure entry points.

8. DISADVANTAGES USING DISTRIBUTED FIREWALL

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.

It is not so easy to implement an intrusion detection system in a distributed firewall environment [7], [10].

9. CONCLUSION

With the increasing speed of data transmission over the network the conventional firewall is not enough for providing authenticated data. So, the term Distributed firewall is come and it provides,

- Complete protection to the network.
- Protects all the clients of the networks from the internal and external attacks.
- Can allow or deny the traffic meant for a particular system based on the policy it has to follow.
- All remote end-user machines can be secured so they can't be used as entry points into the enterprise network.

Because the firewall is distributed across an entire network, the load of processing is further distributed as the network grows, so performance remains high [11].

10. 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 2000, Athens, Greece.

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

[3] Rajendra H. Rathod, V.M. Deshmukh " Roll of Distributed firewall in local network for Data Security" International Journal Of Computer Science And Applications Vol. 6, No.2, April 2013

[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] http://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] Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba, and Masum Hasan "Conflict Classification and Analysis of Distributed Firewall Policies." IEEE Journal in selected areas in communication VOL. 23, NO. 10, October 2005.

[9] Yunus ERDOGAN "Development of a Distributed Firewall Administration tool" November 2008.

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

[11] http://ids.nic.in/technical_letter/TNL_JCES_JU0 L_2013/Data%20Security%20in%20Local%20 Network%20Using%20Distributed%20Firewall.pdf