

# A Survey paper: Data Security in Local Networks Using Distributed Firewalls

Sneha Sahare

M.Tech (Pursuing), Computer Science and Engineering  
Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan (India)  
Jodhpur, Rajasthan (India)  
[mahi.sahare@gmail.com](mailto:mahi.sahare@gmail.com)

Mamta Joshi

M.Tech (Pursuing), Computer Science and Engineering  
Jodhpur Institute of Engineering & Technology, Jodhpur, Rajasthan (India)  
Jodhpur, Rajasthan (India)  
[mamta.joshi1987@gmail.com](mailto:mamta.joshi1987@gmail.com)

Manish Gehlot

M.Tech (Pursuing), Computer Science and Engineering  
Jodhpur National University, Jodhpur, Rajasthan (India)  
Jodhpur, Rajasthan (India)  
[themanishgehlot@gmail.com](mailto:themanishgehlot@gmail.com)

**Abstract**—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. 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 Firewall is a mechanism to enforce a network domain security policy through the use of a policy language, policy distribution scheme enabling policy control from a central point and certificates, enabling the identification of any member of the network policy domain. It secures 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.

In this paper I am dealing with distributed firewall concepts, its evolution, its components, and the policies.

**Keywords:** Network Security, Policy Language, Certificate, Distributed Firewall.

## I. 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. This is a great advantage for individual and corporate as well. But in this case, one should need the 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. 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. 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. For this reason they depend heavily on the topology of the network. More over, firewalls are a mechanism for policy control. That is they permit a sites administrator to set a policy on external access. Just as file permissions enforce an internal security policy, a firewall can enforce an external security policy.

But there are some problems with the conventional firewalls that are as follows.

- Depends on the topology of the network.
- Do not protect networks from the internal attacks.
- Unable to handle protocols like FTP and RealAudio.

- Have single entry point and the failure of this leads to problems.
- Unable to stop spoofed transmissions (i.e., using false source addresses).

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. 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.

## 2. Architecture of Distributed Firewalls

With the concept of distributed firewalls the topological constraints are weakened and a decentralized use of traffic filters as well as components facilitating security requirements as authentication and integrity is favored over one using few special nodes in the overall network. 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, and so on.

**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, 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

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations. Other hosts on a small network, especially the internal endpoint, request to establish communication with the internal endpoint. The connectors use certificates to prove the identity of the remote endpoint, while the certificate is sent to the endpoint by the management center through a policy document mode, which can integrate the remote endpoint connectors and the policy actuators. Thus, in one side the communication between the remote endpoint and the local endpoint is convenient, in the other side the remote endpoint can be provided security protects.

**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.

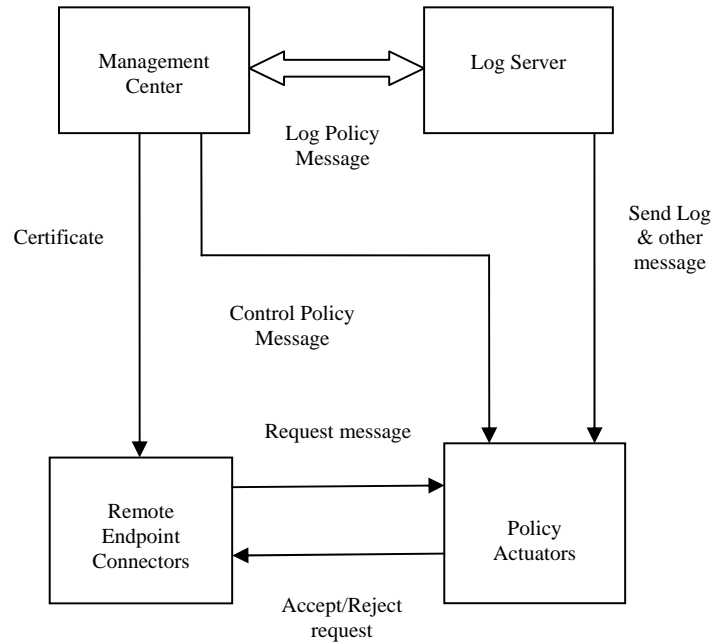


Figure 1: Distributed firewall architecture [16]

## 2.1. Components of Distributed Firewalls

A Distributed Firewall is a mechanism to enforce a network domain security policy through the use of the following:

- Policy Language
- Policy Distributed Scheme
- Certificates

Although the conventional firewalls usually use the network components like IP address as a unique identifier.

### 2.1.1. Policy language

The Policy language is used to create policies for each firewall. These policies are the collection of rules, which guides the firewall for evaluating the network traffic. It also defines which inbound and outbound connections on any component of the network policy domain are allowed.

### 2.1.2. Policy Distribution Scheme

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. Policies are distributed according to one of the following distribution scheme:

- Policies as well as credentials can be pushed to every single end point in the policy domain.
- Policies and credentials can be pulled from a trusted repository during initialization.
- Policies are pulled during initialization of the policy verifier whereas credentials for authentication mechanisms remain on a trusted repository and are requested whenever communication traffic is reaching a node from a yet unknown host.

### 2.1.3 Certificates

There may be the chance of using IP address for the host identification by the distributed firewalls. But a mechanism of security is more important. 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 the certificate is not easily forged. Policies are distributed by means of these certificates.

In implementation of distributed firewall technology, policy languages are translated into some internal format by a compiler. This policy file is distributed to all the protected hosts by the system management software. A

mechanism applies the security policy to incoming packets or connections and the incoming packet accepted or rejected by each host according to policy and the cryptographically verified identity of each sender (Ioannidis).

Different variations may exist in implementation of distributed firewall technology. These variations are called as hybrid firewall, which is a combination of traditional firewall and distributed firewall.

### 3. Advantages of using Distributed Firewalls

- This is the most important advantage of distributed firewalls because they can protect hosts that are not within a topology boundary. Since network security is no more dependant on network topology, it provides more flexibility in defining the security perimeter. Security perimeter can easily be extended to cover remote hosts and networks whenever required.
- Opposing to conventional firewalls, network security is no longer dependent on the single firewall so that the problems like performance Equations bottleneck and traffic congestion are resolved. Besides the load on the conventional firewall is reduced since a large amount of filtering is performed at the end hosts.
- Filtering of protocols like FTP are not easy for conventional firewall, on the other hand it is much easier for distributed firewalls since all of the required information is available at the decision point, which is the end host in general.
- In conventional firewalls there is an assumption that insiders are trustable. However this assumption is the source of several problems. With the distributed firewall architecture, the insiders are no longer trustable. 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 in distributed firewall system. Also the end to end encryption significantly improves the security of the distributed firewalls.[10]

### 4. Disadvantages of Distributed Firewalls

- Compliance of the security policy for insiders is one of the major issues of the distributed firewalls. This problem especially occurs when each ending host have the right of changing security policy. There can be some techniques to make modifying policies harder but it is not totally impossible to prevent it.[10]
- It is not so easy to implement an intrusion detection system in a distributed firewall environment. It is possible to log suspicious connections on local server but these logs need to be collected and analyzed by security experts in central services.[10]

### 5. Related Work

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 form the bottom up in new products. The problem of distributed logging of potentially attacking activity under a central examining mechanism has been addressed by some of the products, and allows for proper response decisions using intrusion detection system. [4]

#### 5.1. Reference Implementations:

In accordance with the concept of distributed firewalls introduces in [2], a reference implementation using IPSec, the KeyNote Policy language [1] and addition to the OpenBSD [1]. Using KeyNote and IPSec allows control of mixed-level policies whereas authentication mechanisms may be applied through the use of public key cryptography but can be based on conventional network address authentication in the absence of it.

#### 5.2. Commercial Products:

- Employing host-based firewall system in its CyberWall PLUS firewall product, Network-1 Security Solutions with a firewall solution which can be classified as a hybrid model of distributed firewalls.
- In addition to the products like virtual private network and policy distribution schemes implementations F-Secure provides a distributed firewall which meets in a combination with other tools available through the vendor.
- Similar to CyberWall PLUS in addition to the mixed level policy enforcement, multiple protocols are supported, as well as the processing of audit logs either locally or on a central host.
- Sygate Technologies, Inc. provides a distributed firewall through the combination of three interacting modules, combined under the bundle Sygate Secure Enterprise.

- In combination with the policy enforcement entity, Sygate Security Agent, and an optional use of cryptography at the network layer, Sygate VPN Enforcer, the product meets the requirements, in addition centralized audit log management and intrusion detection capabilities are supported.
- The STRONGMAN project at the University of Pennsylvania is aiming at simplifying security policy management by providing an application-independent policy specification language that can be compiled to application- specific KeyNote qualifications. These credentials can then be distributed to applications, hosts, and end users and used in an integrated policy framework.
- The most relevant work is that on Symposium on Security and Privacy. The approach in this is the use of a “network grouping” language that is customized for each managed firewall at that firewall. The language used is independent of the firewall and routers used.
- In the approach introduced in [1] they have introduced a three layer system: a high level policy language, an intermediate level language (KeyNote) used by the mechanism, and the actual mechanisms enforcing policy.

#### Acknowledgment

We are indebted to all my elders, lecturers and friends for inspiring me to do my dissertation with immense dedication. With great pleasure and gratefulness, I extend my deep sense of gratitude to Associate Prof. Ashutosh Vyas for giving me an opportunity to accomplish my dissertation under his guidance and to increase my knowledge. Lastly I wish to thank each and every person involved in making my dissertation successful. Thank You.

#### REFERENCES

- [1] Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, Jonathan M. Smith, “Implementing a Distributed Firewall”, CCS '00, Athens, Greece.
- [2] Steven M. Bellovin, “Distributed Firewalls”, November 1999 issue of; login: pp. 37-39.
- [3] W. R. Cheswick and S. M. Bellovin. “Firewalls and Internet Security”: Repelling the Wily Hacker. Addison-Wesley, 1994.
- [4] [Robert Stepanek, “Distributed Firewalls”, rost@cc.hut.fi, T-110.501 Seminar on Network Security, HUT TML 2001.
- [5] Dr. Mostafa Hassan Dahshan “Security and Internet Protocol”, Computer Engineering Department College of Computer and Information Sciences King Saud University mdahshan@ccis.ksu.edu.sa
- [6] David W Chadwick, “Network Firewall Technologies”, IS Institute, University of Salford, Salford, M5 4WT, England
- [7] Anand Kumar “Data security in local networks using distributed firewalls”, Cochin University of science and technology, August-2008.
- [8] Robert Gwaltney, SANS Institute InfoSec Reading Room, “Protecting the Next Generation Network - Distributed Firewalls”, October 7, 2001.
- [9] Lane Thames, “GLOBALIZING INTERNET SECURITY WITH A DISTRIBUTED FIREWALL AND ACTIVE RESPONSE ARCHITECTURE”, April 2008.
- [10] 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.
- [11] Kyle Wheeler, “Distributed Firewall Policy Validation”, December 7, 2004.
- [12] KENNETH INGHAM, STEPHANIE FORREST, “A History and Survey of Network Firewalls”.
- [13] Daniel Wan, “Distributed Firewall” , GSEC Practical Assignment Version 1.2c.
- [14] Lars Strand, “Adaptive distributed firewall using intrusion detection”, 1. November 2004.
- [15] Mohamed G. Gouda, Alex X. Liu, Mansoor Jafry, “Verification of Distributed Firewalls”, 978-1-4244-2324-8/08/\$25.00 © 2008 IEEE.
- [16] Xiong Zeng-gang, Zhang Xue-min, “Research and Design on Distributed Firewall based on LAN”, 978-1-4244-5586-7/10 2010 IEEE.
- [17] William Stallings, “Cryptography and Network Security Principles and Practices”, ISBN-978-81-775-8774-6, PEARSON.
- [18] Atul Kahate, “Cryptography and Network Security”, ISBN-13: 978-0-07-064823-4, ISBN-10: 0-07-064823-9, Mc Graw Hill Higher Education.
- [19] Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security”, ISBN-13: 978-0-07-070208-0, ISBN-10: 0-07-070208-X, Mc Graw Hill Higher Education.
- [20] Vicomsoft- Connect and Protect, “ Firewall Q&A”, 2002 Vicomsoft Ltd – Firewall Software and Internet Security.

#### AUTHORS PROFILE

- [1] Name:- Sneha Sahar  
 Father Name:- Anil sahare  
 Mother Name:- Chhabu Sahare  
 Date of Birth:- 4 March 1987  
 Qualification:- M.Tech(Pursuing), B.Tech  
 Contact Number:- +91-9461004387

[2] Name:- Mamta Joshi  
Father Name:- Rajendra Prasad Joshi  
Mother Name:-Kiran Joshi  
Date of Birth:- 8 December 1987  
Qualification:- M.Tech(Pursuing), B.E  
Contact Number:- +91-7737626057

[3] Name:- Manish Gehlot  
Father Name:- Prem Singh Gehlot  
Mother Name:- Sangeeta Gehlot  
Date of Birth:- 19 March 1987  
Qualification:- M.Tech(Pursuing), B.Tech  
Contact Number:- +91-9024163603