International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec 2018 www.irjet.net p-ISSN: 2395-0072

Data Security in Local Network through Distributed Firewalls: A Review

Shivani Singh[1], Preeti Raj Verma[2]

[1]M.Tech Student, Dept. of Computer Science Engineering, Rama University, Uttar Pradesh, Kanpur
[2]Assistant Professor, Dept. of Computer Science Engineering, Rama University, Uttar Pradesh, Kanpur

---

Abstract - *Our Networks at home, schools, offices, companies and other places are not secured because a number of confidential transaction occur every second and today computers are used mostly for transaction rather than processing of data, so Data security is needed to prevent hacking of data and to provide authenticated data transfer. Network Security can be achieved by Firewall which acts as a filter for unauthorized traffic. But there are some problems with these conventional 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. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate. This paper is 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.*

Key Words: **Network Security, Security Policy, Distributed Firewall, Pull Technique, Push Technique.**

1. INTRODUCTION

A distributed firewall is a mechanism to enforce a network domain security policy through the use of a 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 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. [1].

Distributed firewalls are based on three main points-

Policy Language: The policy language is used to create polices for each of the firewalls. These policies are the collection of rules, which direct the firewall in how to evaluate the network traffic.

System Management Tools: The system management tools are used to distribute the policy to the firewalls and to collect logging and reporting information.

IPSec: IPSEC provides network-level encryption used to secure network traffic and the transmission of policies. It also provides a more important function of providing a way to cryptographically verify the sender of information. Senders can then be uniquely verified by their certificate. It is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation. [2]

Some complications with the conventional firewalls:

1) Depends on the network topology.
2) Do not secure the internal networks attack.
3) Do not handle FTP and Real Audio protocols.
4) There are also single level entry point and the failure of this leads to problems.
5) They do not stop "spoofed" transmissions.
6) Unable to logging all of the network's activity.
7) Unable to dynamically open and close their networking ports. [3]

2. ARCHITECTURE OF DISTRIBUTED FIREWALL-

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:

A. 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.

B. Policy actuator: Policy actuator is installed in each host or gateway to receive the security policy issued by the management center, and to explain and 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.

C. 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.

D. 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.[4]

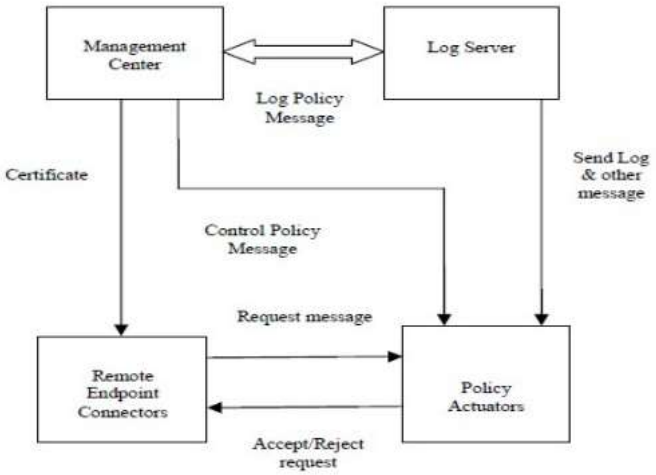

Fig 1- Distributed Firewall Architecture[5]

3. COMPONENTS OF DISTRIBUTED FIREWALL

A. Central management system- Central Management, a component of distributed firewalls, makes it practical to secure enterprise-wide servers, desktops, laptops, and workstations. Central management provides greater control and efficiency and it decreases the maintenance costs of managing global security installations. This feature addresses the need to maximize network security resources by enabling policies to be centrally configured, deployed, monitored, and updated. From a single workstation, distributed firewalls can be scanned to understand the current operating policy and to determine if updating is required.

B. Policy distribution- The policy distribution scheme should guarantee the integrity of the policy during transfer. 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

C. Host-end implementation- The security policies transmitted from the central management server have to be implemented by the host. The host end part of the Distributed Firewall does provide any administrative control for the network administrator to control the implementation of policies.

4. Working with distributed firewalls

Most distributed firewalls run in kernel mode and sit at the bottom of the OSI stack. The firewall evaluates all network traffic whether it is from the Internet or from the internal network. This protects the system much in the same ways as traditional firewall protects the network. After the firewall is installed on all network endpoints, a central policy is developed. This policy is written using the policy language and then compiled in a format to be transferred to each firewall. The system management tools are then used to transfer the policy to each firewall. Because the firewalls are in different locations throughout the network and may be on a machine that changes locations, they cannot depend on the network topology to determine the sender of the network traffic. For this they use the certificates provide by IPSEC. These certificates uniquely identify the sender and don't depend on the network topology. The firewall then evaluates the traffic based on the central policy and decides to allow or deny it. The firewall can also then transfer logging information to a central location where it can be used for reporting.

4.1 Policies

One of the most often used term in case of network security and in particular distributed firewall is policy. It is essential to know about policies. A "**security policy**"defines the **security** rules of a system. Without a defined **security policy**, there is no way to know what access is allowed or disallowed. A simple example for a firewall is

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

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.

4.2 Pull technique

The host while booting up, pings to the central management server to check whether the central management server is up and active. It registers with the central management server and requests for its policies which it should implement. The central management server provides the host with its security policies. A conventional firewall could do the same, but it lacks important knowledge about the context of the request. End systems may know things like which files are involved, and what their security levels might be. Such information could be carried over a network protocol, but only by adding complexity.

4.3 Push technique

The push technique is employed when the policies are updated at the central management side by the network

administrator and the hosts have to be updated immediately. This push technology ensures that the hosts always have the updated policies at any time. The policy language defines which inbound and outbound connections on any component of the network policy domain are allowed, and can affect policy decisions on any layer of the network, being it at rejecting or passing certain packets or enforcing policies at the Application Layer. [6]

5. Distributed Firewall Implementation

5.1 Language: used to express policies and resolving requests (Keynote systems). Using keynote; IPSec allows control of mixed level policies where authentication mechanism is applied through public key cryptography.

5.2 Keynote system: is a language to describe security policies (RFC 2704), all field names are case-insensitive and Blank lines are not permitted within an assertion Policies and Credentials have same basic syntax, are "delegated" and MUST be signed.[7]

Trust Management is a relatively new approach to solving the authorization and security policy problem. Making use of public key cryptography for authentication, trust management dispenses with unique names as an indirect means for performing access control. Instead, it uses a direct binding between a public key and a set of authorizations, as represented by a safe programming language. This results in an inherently decentralized authorization system with sufficient expressibility to guarantee flexibility in the face of novel authorization scenarios. Give response, Verifier Requester, Request, Key, Sig, Keynote, Gather information local policy Pass (remote credentials) information, Evaluate Application Interactions with Keynote. The Requester is typically a user that authenticates through some application dependent protocol, and optionally provides credentials. The Verifier needs to determine whether the Requester is allowed to perform the requested action. It is responsible for providing to Keynote all the necessary information, the local policy, and any credentials. It is also responsible for acting upon Keynote response. One instance of a trust-management system is Keynote. Keynote provides a simple notation for specifying both local security policies and credentials that can be sent over an untrusted network. Policies and credentials contain predicates that describe the trusted actions permitted by the holders of specific public keys (otherwise known as principals). Signed credentials, which serve the role of "certificates," have the same syntax as policy assertions, but are also signed by the entity delegating the trust. Applications communicate with a "Keynote evaluator" that interprets Keynote assertions and returns results to applications. However, different hosts and environments may provide a variety of interfaces to the Keynote evaluator (library, UNIX daemon, kernel service, etc.). A Keynote evaluator accepts as input a set of local policy and credential assertions, and a set of attributes, called an "action environment," that describes a proposed trusted action associated with a set of public keys (the requesting principals). The Keynote evaluator determines whether proposed actions are consistent with local policy by applying the assertion predicates to the action environment. The Keynote evaluator can return values other than simply true and false, depending on the application and the action environment definition. An important concept in Keynote (and, more generally, in trust management) is "monotonicity". This simply means that given a set of credentials associated with a request, if there is any subset that would cause the request to be approved then the complete set will also cause the request to be approved. This greatly simplifies both request resolution (even in the presence of conflicts) and credential management. Monotonicity is enforced by the Keynote language (it is not possible to write non-monotonic policies).

6. CONCLUSIONS

Most of the systems, the network security is achieved by firewall and acts as a filter for unauthorized traffic. But there are some problems with these traditional firewalls and few more problems lead to the evolution of Distributed Firewalls. It secures the network by protecting critical network endpoints, exactly where hackers want to penetrate.

The aim of this paper is the 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.

7. REFERENCES

1. http://www.123seminarsonly.com/Seminar Reports/029/50774016-Data-Security-in-Local-Network-Using-Distributed Firewall.pdf

2. JayshriV.Gaud and MahipM.Bartere "Data security based on LAN using distributed firewalls" [International Journal of Computer Science and Mobile Computing. March 2014]

3. http://docshare.tips/approach-of-data-security-in-local-network-using-distributed-firewalls-5875e423b6d87fb5398b4624.html

4. SnehaSahare, Mamta Joshi and Manish Gehlot "A survey paper data security in local networks using distributed firewalls" [International Journal on Computer Science and Engineering (India); 09 Sep 2012]

5. HiralB.Patel, Ravi S. &Jayesh A.P. "Approach of data security in local network using distributed firewalls" [International Journal of P2P Network Trends and Technology- Volume1Issue3-2011]

6. Prof.V.M.Deshmukh and RajendraH.Rathod "Roll of distributed firewalls in local network for data Security" Badnera-Amravati, India [International Journal of Computer Science and Applications Vol. 6, No.2, Apr 2013].

7. Suraj J. Warade, PritishA.Tijare and Swapnil. N. Sawalkar "A Review Data Security in Local Network using Distributed Firewall" [National Conference on Emerging Trends in Computer Technology - 2014]