Data Security in Local Network for Mobile using Distributed Firewalls

Miss. Soumya Patil[1], Dr. Sunita S. Padmannavar[2]

[1]PGStudent, Department of MCA, KLS Gogte Institute of Technology, Udyambag, Belagavi, India.
[2]Asst. Prof, Department of MCA, KLS Gogte Institute of Technology, Udyambag, Belagavi, India.

---***---

Abstract - *Networks and computers 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. Data security can be achieved by Firewall; a firewall is typically placed at the edge of a system and acts as a filter for unauthorized traffic. firewalls is a device or set of instruments designed to permit or deny network transmissions based upon a set of rules and regulation is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass or during the sensitive data transmission.*

Key Words: Local Networks, Security Policy, Firewall, Distributed Firewall, FTP.

INTRODUCTION

A firewall is a collection of components, interposed between two networks, that filters traffic between them according to some security policy. Distributed firewalls are host-resident security software applications that protect the enterprise network's servers and end- user machines against unwanted intrusion. They offer the advantage of filtering traffic from both the Internet and the internal network. This enables them to prevent hacking attacks that originate from both the Internet and the internal network.

ARCHITECTURE OF DISTRIBUTED FIREWALLS

Growth in internet access speeds, coupled with increasingly compute-intensive protocols that firewalls have to analyse, have resulted in firewalls becoming congestion points.

Distributed firewalls help solve this problem by using processing power across the network, not just on a single cluster or machine where a firewall is installed.

A distributed firewall is a host-resident security software application, which protects the network as a whole against unwanted intrusion. Deployed alongside more traditional firewalls, distributed firewalls can add another layer of protection to a network while still maintaining high throughput for legitimate network traffic.

In addition, centralized firewalls are based on a model that assumes attacks are coming from outside a network. They apply a "perimeter defence" model where a firewall guards only against malicious traffic coming from outside the network.

This model fails, however, if an attack comes from inside the network – an all-too-common occurrence given the huge variety of ways that users can connect to an internal network, including wireless access and VPN tunnels. Traditional firewalls typically can't effectively guard against attacks coming from sources like these, but a distributed firewall can add another layer of defence against this type of attack.

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 fulfil the requirements of efficient system and network administration. The whole distributed firewall system consists of four main parts:

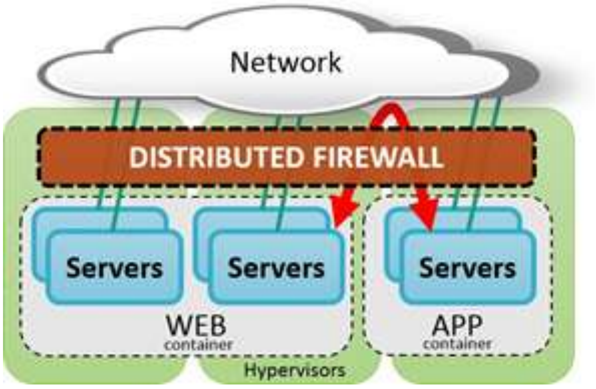

Figure 1. Architecture of Distributed

Firewall Standard Set of Capabilities

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.

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 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.

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.

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.

There are three components of distributed firewalls

i. **Policy language:** Policy language used to create policies for each firewall. These policies are the collections of rules, which guide the firewall for evaluating the network traffic and also defines which inbound and outbound connections are allowed or rejected.

ii. **Policy distribution scheme:** Policy distribution scheme is used to enable policy control from central point. This policy is consulted before processing the incoming or outgoing messages. It should guarantee the integrity of the policy during transfer. It can be either directly pushed to end systems, or pulled when necessary with the implementation.

iii. **Certificate:** Certificate enables making decisions without knowledge of the physical location of the host. There may be the chance of using IP address for host identification by the DFW, it is preferred to use certificate to identify hosts. IPS provides cryptographic certificates, unlike IP address which can be easily spoofed, the digital certificate is much more secure and the authentication of certificate is not easily forged.

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.

PULL TECHNIQUE

The hosts 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.

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 anytime. 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.

ADVANTAGES OF DISTRIBUTED FIREWALLS

1. Topological independence is one of the main advantages

2. As mentioned earlier, filtering of certain protocols such as FTP is not so easy on a conventional firewall. Such kind of a process is much easier on distributed firewalls since all of the required information is available at the decision point, which is the end host in general.

3. The distributed firewalls network protect from hackers attacks.

DISADVANTAGES OF DISTRIBUTED FIREWALLS

1. 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.

2. Intrusion detection systems are less effective with distributed firewalls because complete network traffic is not on the single point.

3. It is not so easy to implement an intrusion detection system in a distributed firewall environment.

CONCLUSION

The data is secured by using the distributed firewalls these are provides security. Data Security along with a fast technological change is a demanding field. This overview shows that Data Security in itself must be seen as a whole. The adopted network security policy forms the basis. A proper choice of systems, protocols, standards and techniques gives the guidelines for a more secure networking.

REFERENCE

[1] Jayshri V.Gaud and Mahip M.Bartere "Datasecurity based on LAN using distributed firewalls", International Journal of Computer Science and Mobile Computing.,March 2014

[2] Pritish A. Tijare, Suraj J. Warade and Swapnil. N. Sawalkar "Data security in local network using distributed firewalls",National Conference on Emerging Trends in Computer Technology (NCETCT-2014)

[3] https://en.wikipedia.org

[4] https://www.barracuda.com/glossary/distributed-firewall