Data Security in Local Networks Using Distributed Firewalls

R. Maruthaveni[1], R. Latha[2]

[1, 2]Assistant Professor, Department of Computer Science Dr. SNS Rajalakshmi College of Arts and Science, Saravanampatti, Coimbatore – 49, India

Abstract: ***Today, computer and networking are inseparable. A number of confidential transactions occur very second and today computers are used mostly for transmission rather than processing of data. So Network Security is needed to prevent hacking of data and to provide authenticated data transfer. Network Security can be achieved by Firewall. Conventional firewalls rely on the notions of restricted topology and controlled entry points to function. Restricting the network topology, difficulty in filtering of certain protocols, End-to-End encryption problems and few more problems lead to the evolution of Distributed Firewalls. 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. Distribute firewall solves these problems and protecting critical network end points where hackers want to penetrate. 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

1. 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. Moreover, firewalls are a mechanism for policy control. 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.

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, which88 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 dependants 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.

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

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.

5.1. Reference Implementations

In accordance with the concept of distributed firewalls introduces in [2], a reference implementation using IPSec, the Key Note Policy language and addition to the Open BSD. Using Key Note 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 Cyber Wall 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 WKURXJK WKH YHQGRU 6IP ILQDU WR &\EHU : DOO 3/ 8 6 ILQ 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.

6. Conclusion

We have discussed the concept of a distributed firewall. Under this scheme, network security policy specification remains under the control of the network administrator. Its enforcement, however, is left up to the hosts in the protected network. Security policy is specified using KeyNote policies and credentials, and is distributed (through IPsec, a web server, a directory-like mechanism, or some other protocol) to the users and hosts in the network. Since enforcement occurs at the endpoints, various shortcomings of traditional firewalls are overcome. Security is no longer dependent on restricting the network topology. This allows considerable flexibility in defining the “security perimeter,” which can easily be extended to safely include remote hosts and networks (e.g., telecommuters, extranets). Since we no longer solely depend on a single firewall for protection, we eliminate a performance bottleneck. Alternately, the burden placed on the traditional firewall is lessened significantly, since it delegates a lot of the filtering to the end hosts. Filtering of certain protocols (e.g., FTP) which was difficult when done on a traditional firewall, becomes significantly easier, since all the relevant information is present at the decision point, i.e., the end host.The number of outside connections the protected network is no longer a cause for administration nightmares. Adding or removing links has no impact on the security of the network. “Backdoor” connections set up by users, either intentionally or inadvertently, also do not create windows of vulnerability.

7. Future Scope

The update mechanism has the following characteristics that, new policy is formed and appended at the initiation of the existing policy. New updated policy is created without almost any similar rules. After the firewall updating and new configuration, the proposed implemented firewall has the distinctiveness that the firewall policies rules are based on the defined and develop rules’ manage the firewall to be utilized. For accuracy in detection and removing possible misconfiguration from the updated policy, it seems rectification algorithms, which determine potential errors, and also investigation in redundancy and shadowing is required.

References

[1] Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin, Jona than M. Smith, “Implementing a Distributed Firewall” CCS ’00, Athens, reece.
[2] Steven M. Bellovin, “Distributed firewalls November 1999 issue
[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
[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 InFo Sec 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 F irewalls”, International Journal of P2P Network Trendsand Technology- Volume1 Issue3- 2011.
[11] Kyle Wheeler, “Distributed Firewall Policy Validation”, December 7, 2004.
[12] Kennetingham, stephanie forrest, “A History and Survey of Network Firewalls”.
[13] Daniel Wan, “Distributed Firewall” , GS EC Practical Assignment Version 1.2c.
[14] Lars Strand, “Adaptive distributed Firewall using intrusion detection”,
[15] Mohamed G. Gouda, AlexX . Liu, Mansoor Jafry, “Verification of Distributed Firewalls”,
[16] Xiong Zeng - gang, Zhang Xue- min, “Research and Design on Distributed Firewall based on LAN”,
[17] William Stalling, “Cryptography and Network Security Principles and Practices”,
[18] Atul Kahate “Cryptography and Network Security”,Mc Graw Hill Higher Education.
[19] Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security McGraw Hill Higher Education.

[20] Vicomsoft - Connect and Protect, “Firewall Q&A”, 2002 Vicoms of Ltd – Firewall Software and Internet Security.

Author Profile

Mrs. Maruthaveni R is working as Assistant Professor, Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore – 49, India

Mrs. Latha R is working as Assistant Professor in Department of Computer Science, Dr.SNS Rajalakshmi College of Arts and Science, Coimbatore - 49, India