International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 3, March - 2013

Enhanced Behavior Of DF Using Intrusion Detection

Mr. S. V. Athawale[1], Himgauri Shejwalkar[2,] Priya Sankpal[3], Ankita Naik[4,] Ashwini Pawar[5]

[1]Asst. prof.(Conputer Engineering,AISSMS College of Engineering, India)

[2] (Conputer Engineering,AISSMS College of Engineering, India)

Abstract:

The Internet Firewall is one of the key technologies in network security. Due to the rapidly increasing network attacks and firewalls have become important elements not only in enterprise networks but also in small size and home networks. However firewalls do not support protocols like FTP. Solution to this is distributed firewall. Distributed Firewall allows centralized filtering of traffic entering and exiting the protected network.

For implementation of distributed firewall, we use security policies that can describe which connections are acceptable, which are denied an authentication mechanism, and a policy distribution scheme. A distributed firewall security policy is a list of ordered filtering rules. These rules define the actions performed on packets that satisfy particular conditions. A rule is composed of set of filtering fields. The effectiveness of firewall security is dependent on providing policy management techniques and tools that administrators of network can use to verify, purify and analyze the correctness of written firewall filtering rules.

Keywords: distributed, authentication, policy.

I. INTRODUCTION

A firewall is a system or group of systems (router, proxy, or gateway) that implements a set of security rules to enforce access control between two networks to protect "inside" network from "outside" network. Firewalls are devices or programs that control the flow of network traffic between networks or hosts. Firewalls are often placed at the perimeter of a network. These can be said to have an external and internal interfaces, with the external interface being the one on the outside of the network .With hacking attempts, the cost of security breaches and the importance of suspicious computer security in general all on the increase. Many enterprise networks use firewalls to restrict connectivity to and from the internal or outer networks used to service personnel functions. By making use of firewalls, we can control connectivity to these fields as described in [2].

Traditional firewalls rely on a strict outside/inside topology where the gateways enforce some sort of traffic filtering. Some claims that with the growing connectivity of the Internet, the traditional firewall has been old-fashioned. High speed links, vibrant topology, end-to-end encryption, threat from internal users are all problems that must be addressed as per [6].

Traditional firewalls can become a bottleneck .Certain protocols like Real-Audio, FTP are difficult for firewalls to process. It assumes inside users are “confidential” .Also, multiple entry points make firewalls hard to manage.

Firewalls have a number of advantages. As per [6] they can prevent incoming requests to inherently insecure services, for example we can prohibit login, or RPC services like NFS. They can control access to other services. They filter the service operations (both incoming and outgoing). They are more cost effective than securing each host on the corporate network since there are only one or a few firewall systems for concentrating. They are most secure than securing each host of network due to, the complexity of the software on the host. This makes it more easier for security loop holes to appear.

([5], [8], [9]) Describes that a distributed firewall is bringing the firewall to the end hosts. By doing this, it is possible to get the firewall into a mobile network and other shortcomings of the traditional firewall which are described above. Use of distributed firewall make the management of its policy centralized, but its policy is distributed. Domain security policy through the use of a rule language, a strategy distribution scheme enabling policy control from a central point and certificates, enabling the detection of any member of the network policy domain.

Intrusion detection and prevention

Intrusion detection systems [3] provides a way to defend against the various threats to which hosts and networks are exposed to by detection of the actions of attacks or attackers tools in a network or host based manner with anomaly detection techniques. Once intrusion detection system detects a suspicious action, it immediately generates an alert which contains information about the destination, source and estimated type of the attack.

Traditionally intrusion detection system relay on extensive knowledge and information of security experts, on their familiarity with the computer system to be protected.

An Intrusion Prevention System (IPS) [1] is a network software or device that helps to discover and block network threats by assessing each packet based on the network protocols in the network layer on the context of the tracking and communication of each session. IPS is a proactive defense mechanisms that are designed to detect malicious packets within normal network congestion and stop intrusions and block the traffic automatically before it cause any damage to a system rather than simply raising an alert of the malicious things has been detected.

II. RELATED WORK

A considerable amount of work has been done in the area of firewall and policy-based security management. We have focused our study on the related work related to packet filter modeling, conflict discovery and rule analysis, and distributed firewall policy management. Several models have been proposed for filtering rules. The other model, uses bucket filters indexed by search trees. Geometric model is used to represent 2-tuple filtering rules. Because these models were designed particularly to optimize packet classification in high speed networks, we found them too complex to use for firewall policy analysis. Interval diagrams are used to compact firewall rules. However, it requires pre-processing of firewall rules to resolve any rule overlap, and therefore it cannot be used for our anomaly analysis.[6]

III. PROPOSED SYSTEM

For implementing distributed firewall we need initial packet filtering rules and security policy scheme. Three important things are considered: access policy rules, Network Address Translation (NAT) policy, and routing rules.

Access policy rules controlling access to filter traffic, and from the firewall machine and the machines behind it. The policy rule consists of one or more expressions in the NetScaler expressions language. The NetScaler language syntax is object-oriented programming language, powerful that enables you to precisely designate the traffic that you want to process with a specific profile.

For users, who are not completely familiar with the NetScaler appliances which uses a web based interface. That configuration utility provides two tools: the Add Expression dialog box and Prefix menu . Both help you to write expressions that select exactly the traffic that you want to develop. Qualified users who are familiar with the syntax prefer to use the NetScaler command line to organize their NetScaler appliances. We are going to use Java oops to design distributed behavior of a firewall because we are focusing on software based firewall not hardware.

Packet filtering

Packet filtering is the process of blocking or passing packets at a network interface based on source address and destination addresses, protocols or port numbers. Packet filtering is part of a firewall program for protecting a small size network from unwanted and unauthorized intrusion. In distributed firewalls packet filtering is done by a computer program called a packet filter. The packet filter program examines the header of each packet based on a specific set of rules and on that basis it decides to prevent it from passing (DROP) or allow it to pass (ACCEPT) as described in([7],[4]). [7] consists of following 3 ways in which a packet filter can be configured.

- Method 1: In this method, the firewall filter accepts only those packets which are safe. This is the more secure mode. But it can cause inconvenience if legitimate packets are inadvertently dropped.

- Method 2: In this method, the firewall filter drops only the packets that it is certain are not safe, accepting all others. This mode is the least secure. It causes less inconvenience, particularly in casual Web browsing.

- Method 3: In this method, if the filter detects the packet for which its rules do not provide instructions, that packet can be quarantined. This can be inconvenient if it causes numerous dialog boxes to appear during Web browsing.

Policies

([7], [10]) Describes one of the most often used term in case of network security and in particular distributed firewall is a policy. It is necessary to know about policies. A network security policy defines the security rules of a system. These rules are very important because system's security depends on the rules we write. Without policies there is no way to know what access is authorized and allowed or which access is denied.

Modeling a distributed firewall rule relations is important for analyzing the firewall policy and design management techniques such as policy editing and anomaly discovery. In this section, we formally describe our model of firewall rule relations and we describe a tree-based representation of firewall policies.

Formalization of Firewall Policy Relations

To build a useful model for filtering rules, we need to identify all the relations that are related to packet filtering. We define all the possible relations that may exist between filtering rules and also we show that no other relation exists. These relations are identified on the basis of comparing the fields of filtering rules that are independent of the rule actions as in [6].

Firewall Policy Representation

[6] represent the firewall policies by a single rooted tree which is also known as the policy tree. This tree model provides simplified representation of the filtering rules and at the same time it allows for easy discovery of anomalies and relations among these rules.

In this policy tree each node represents a network field. Also branch at this node represents a possible value of the associated field. The tree flow or path starting from the root node and ending at a leaf represents a rule in the policy and vice versa. Rules having the same field value at a particular node, shares the same branch representing that value.

IV. CONCLUSION

Aim of this paper is to propose systems that will perform better than those in the current literature survey. Also to provide solution for unwanted attacks using distributed firewall. In this paper we have tried to explain the internet problems and solution of that problem with the help of distributed firewalls. Also we explained packet filtering and policy anomalies needed for implementation of distributed firewall.

REFERENCES

[1] Dinesh Sequeira, “Intrusion Prevention System – Security’s Silver Bullet?” SANS Institute InfoSec Reading Room,2002.

[2] Khaled Salah, Khalid Elbadawi, Raouf Boutaba, ”Performance Modeling and Analysis of Network Firewalls.” in IEEE transaction on network and service management, vol. 9, no. 1, March 2012.

[3] Lars Strand,” Adaptive Distributed Firewall Using Intrusion Detection” In UniK University Graduate Center University of Oslo, November 2004.

[4] Hazem Hamed, Adel El-Atawy, Ehab Al-Shaer, “On Dynamic Optimization of Packet Matching in High-Speed Firewalls.” In IEEE transaction on selected areas in communication, vol. 24, no. 10, October 2006.[4]

[5] Alex X. Liu, Member, IEEE, and Mohamed G. Gouda, “Diverse Firewall Design.” In IEEE transaction on parallel and distributed systems, vol. 19, no. 9, September 2008.[5]

[6] Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba, Masum Hasan, “Conflict Classification and Analysis of Distributed Firewall Policies.” In IEEE transaction in communication, vol. 23, no. 10, October 2005.[10]

[7] Karen Scarfone,Paul Hoffman, “Guidelines on Firewalls and Firewall Policy.” Recommendations of the National Institute of Standards and Technology.

[8] Distributed Firewalls [online] available: https://www.cs.columbia.edu/~smb/papers/distfw.html

[9] Distributed Firewall [Online] Available:
http://www.scribd.com/doc/12885424/Distributed-Firewall

[10] Discovery of Policy Anomaly in Distributed Firewalls [Online] Available:
http://www.ieee-infocom.org/2004/Papers/54_3.PDF