Distributed Firewall with Intrusion Detection System

Linquan Xie
School of Science, Jiangxi University of Science and Technology, 341000 Ganzhou, China
Email: lq_xie@163.com

Fei Yu[1], Chen Xu[1, 2]
[1] Jiangsu Provincial Key Laboratory for Computer Information Processing Technology, Soochow University, 215000 Soochow, China
[2] School of Information Science and Engineering, Hunan University, 416000 Changsha, China
Email: hunanyufei@126.com

***Abstract*—With the growth of Internet, network security has received significant attention over pass ten years due to the increasing threat of hacker attacks. To achieve security goals, most corporate environments have deployed firewalls to block the intrusion. However, traditional firewalls only provided static filleting analysis so that they can not analyze the content of data packet for providing dynamic security requirement. In order to address this issue, in this paper, we integrate the traditional firewalls with intrusion detection technologies. The proposed can provides dynamic security defense by atomically updating the policies based on the detection condition.**

***Index Terms*—Firewall; Intrusion Detection; Network Security.**

I. Introduction

Nowadays, with the development of network technologies and applications, security problem has become a hot topic because there are more and more economic losses due to the hacker attacks. Although there are many of security technologies to protect network attacks such as firewalls, intrusion detection systems (IDSs), etc, different security technologies are designed to address certain security issues so that such technologies can not cooperate with each other for protecting various attacks together. Even worse, they might defense to each other. Based on some researches, there are annual economic losses due to the hacker attacks. For example, analysts estimate that 50% of large corporations have seen a computer break-in over the past years [3]. According to the [4-5], during 1995-1996, annual financial losses are the range from hundreds of millions of dollars to 30+ billion dollars due to the various attacks. From the data, we get to know that the increasing of network application has made the security question more complicated than pass so that the single intrusion detection systems and firewalls can no meet the current requirement of network security. For example, the IDSs do not prevent an intrusion before it happens in a secure system [1-2] due to the IDs only detect known attacks and viruses.

Firewalls are the technologies of access control by controlling the traversal of packets across the boundaries of a secured network based on a specific security policy defined in advance by the network administrator. A firewall security policy is a list of ordered filtering rules that define the actions performed on matching packets. Typically, a firewall rule is composed of filtering and operation information such as source and destination address, protocol type, source and destination IP addresses and ports, as well as an action field. However, the filtering rules are established in advance. Thereby, traditional firewall can not adjust the static filtering rules to resist to the real-time attacks. In order to achieve the performance, the traditional firewalls only check the packet header but not examine the details of the content and the protocol. Thereby, as long as the data packet is not matched the filtering rules, then the firewalls will let the packet come in. Intrusion Detection Systems can make up for the shortcomings of absence of content checking of firewall.

IDSs try to detect any suspicious action by monitoring the events occurring in a computer system or network, and then by analyzing them for signs of intrusions. When something specially happens, the IDSs then notify the network administrator [6]. Generally, IDSs have three essential security functions: monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. However, one main weakness of instruction diction system is that there are high errors and miss rate so that these issues have been plagued by the security administrator [7].

Although the firewalls and intrusion detection techniques are be applied to protect network attacks, such two techniques are usually operated as standalone system to protect an isolated subsystem or network only. That is to say, there is low possibility for coordinated operation

Manuscript received February 20, 2011; revised March 22, 2011; accepted June 25, 2011.

doi:10.4304/jcp.7.12.3110-3115

between the firewalls and IDSs. Thereby, in order to against sophisticated attacks and upcoming threats, there should combine firewall and IDSs so that they can cooperate with each other. In this paper, we propose a novel firewall integrated with the intrusion detection technologies. The main system function of the novel firewall will be presented in this paper.

The rest of the paper is organized as follows: the next Section we briefly reviews the backgrounds and existing techniques of firewall. Firewalls with intrusion detection techniques are proposed in details in Section 3. Finally, we draw a conclusion in section 4.

II. The Firewalls Techniques

In this section, we briefly review the existing techniques and the backgrounds of firewalls. A firewall is a technique that is ideally a separate computer to divide the internal networks from Internet based on a specific security policy. The first firewalls were simple packet filter for controlling access between networks. Till to new, firewalls are designed to provide numerous security functions [11].

1) Track and maintain state between multiple sessions.

2) Authenticate users using tokens or one-time password.

3) When the traffic password the firewall, they should be encrypted decrypted.

4) Provide secure private channel and virtual network in insecure networks.

5) Not only support TCP, but also support low overhead protocol for real needs
such as UDP.

6) Ensure its own security is not compromised.

Figure 1 shows a typical architecture that separate an organization's network (internal networks) from the Internet.

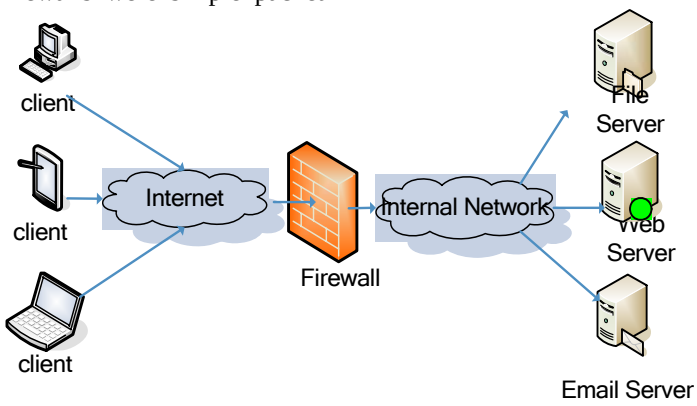

Figure 1. Firewall Archietecure

A. The Packet Filter Firewall

The first generation of firewall is the Cisco's IOS software division [12], which is also called Packet Filter Firewalls. Packet Filter Firewalls are the most basic, fundamental type of firewall. . The packet filter firewalls are the techniques that analyze the network traffic to judge the persimmons based on the packet header according a series of pre-defined rules. When the packet filter firewall receives a packet of information, the filter compares the packet to the pre-configured rules set to accept or deny the traffic. In general, Packet filters usually permit or deny network traffic based on the following attributes.

Source and destination IP addresses.

Protocol, such as TCP, UDP, or ICMP

Source and destination ports and ICMP types and codes

Flags in the TCP header, such as whether the packet is a connect request

Direction (inbound or outbound)

Which physical interface the packet is traversing

The main advantage of this kind of firewall is speed, flexibility and simplicity. Also, the installation, modification is easy to implement.

B. The Circuit Level Gateways Firewall

The Circuit Level Gateways firewalls are also called Proxy Service firewalls, which is the second generation of firewall architectures and is first researched by Dave Presotto and Howard Trickey of AT&T Bell Labs around 1989-1990[13]. Compared to packet filter firewalls, the Circuit Level Gateways firewalls doesn't simply allow or disallow packets but determines whether the connection is valid according to observing handshaking between packets. For example, the verification may be based upon:

destination IP address and/or port
source IP address and/or port
time of day
protocol
user
password

The main advantages of circuit level gateways are that these kind firewalls are common faster than application layer firewalls due to the fact that they are fewer evaluations.

C. The Application-Gateway Firewall

An application-gateway firewall are called third generation of firewall architectures, which we developed

by Gene Spafford of Purdue University, Marcus Ranum, and Bill, Cheswick of AT&T Bell Laboratories[13] during the late 1980s. Application-gateway firewall operates on seven layers of the OSI mode and thus it is much more secure and reliable compared to packet filter firewalls. It acts as a proxy for applications, performing all data exchanges with the remote systems in their behalf. An application firewall can filter higher-layer protocols such as FTP, Telnet, DNS, DHCP, HTTP, TCP, UDP and TFTP (GSS). It can allow or disallow traffic according to very specific rules, for instance permitting some commands to a server but not others, limiting file access to certain types, varying rules according to authenticated users and so forth. Application-level gateways are generally regarded as the most secure type of firewall. However, the system setup may be very much complex than other type firewall.

III. Distributed Firewall with Intrusion Detection System

In this section, the present the architecture of the novel firewalls. One big disadvantage of the traditional firewall is that the firewalls rely on the static filtering rule, defined by an administrator in advance, to defense passively. Thereby, in order to achieve more security requirement, there should integrate the intrusion detection technologies into the firewall for providing dynamic security policy because the IDSs can provide dynamic defense technologies by analyzing the network traffic real-time. If there something specially happens, the IDSs call the alarm function for notifying the network administrator. For achieving such requirement, we can use the combine technologies by this way that if the something abnormal happens, then IDSs modify existing filtering rule of the firewall by adding the new defense rules to the original ones. Figure 1 shows the system model of the firewall with IDS function. Firewall and IDS are the core component in the whole system, which is placed at the core layer. Above the core layer, there lie at the application layer, which receives the network traffic and deliver it to the core layer for further process.

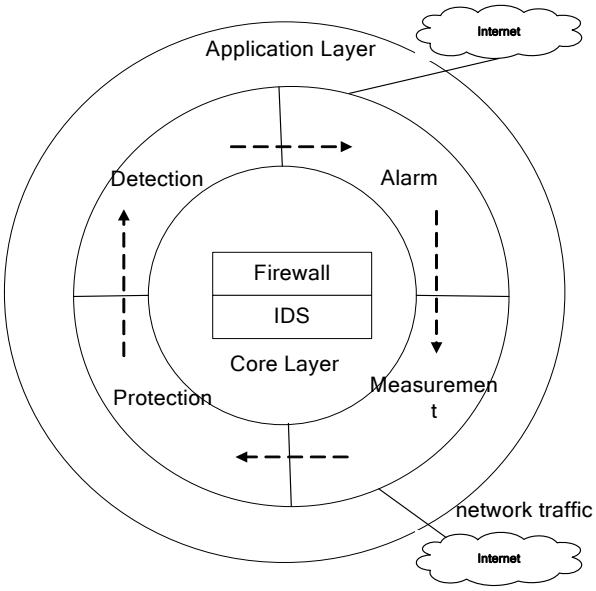

Figure 2. The Novel Firewall Model

A. The System Architecture

The system architecture is presented in Figure 2. Note that the firewall and the intrusion detection modules cooperate with each other for protecting network attacks. In the sub Section, we describe each module function of the system.

(1) Firewall

The firewalls module is responsible for analyzing the network traffic to judge the persimmons according to a series of rules defined in the Policy Repository.

(2) Intrusion Detection Module

Having receiving the packet from the firewall, the module then analyzes the network traffic real-time. Note that the traditional firewall module doesn't analyze the content of the data packet. Similar to traditional IDSs, this module monitors can analyze user and system activity by analyzing the content of the packet. Having detecting possible attacks, the Intrusion Detection Module calls the Policy Hander to judge whether there is should add or modify a filtering rule for protecting the adversary to attack. Note that once adding filtering rules, which defined in the next sub section 3, then the firewall will block the packet, which is matched in the Policy Repository. The firewall with intrusion detection technologies can enhance network protection by carrying out the dynamic defense mechanism. Also, the module records the attack events into the log database.

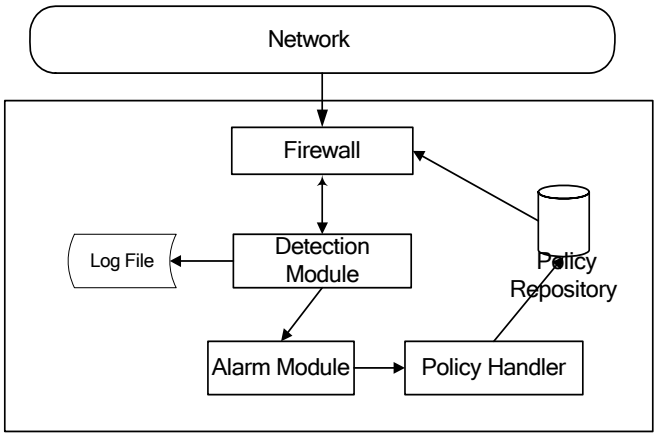

Figure 3. The System Architecture

(3) Policy Repository

The Policy Repository defined all the filtering rules that the systems accept or deny the packet. Similar to the traditional firewall, the rules are presented in the following format.

<order> <protocol> <src_ip> <src_port> <dst_ip> <dst_port> <action>

The order of the rules presents the relative position of one rule. The protocol specifies the transport protocol of the packet such as IP, TCP and UPD, etc. src_ip and src _port are the source's network addresses and port number, respectively. Likewise, dst_ip and dst _port are the destination IP addresses and ports number. The port can be either a single specific port number, or any port number presented by "any". The action can be either "accepts" or "deny" [8]. However, one big weakness of traditional firewall is that the policy is static, which is established in advance. Thereby, the traditional firewall can not resist to real-time attacks. For addressing these issues, we, in this paper, combine the firewall with IDSs to provide dynamic rules. That is, there are no longer store static rules into the Policy Repository, but the dynamic ones. Note that it is the Policy Handler deal dwith the policy modification.

(4) Policy Handler

The Policy Handler interprets the detection policies which may be triggered by the Log File. Note that the module has the privilege to update the policy rules of the firewalls based on the detection results got from the Detection module. Possible actions are notifying, or reconfigure.

(5) Log Database

This module records the event of packet filtering, intrusion detection, and the operation of the firewalls. The log database provides the basic data for an administrator to analyze, audit, and check the effect of proposed firewall.

(6) Alarm Module

Having detecting the networks security, the alarm module notifies the administrator right now by the some communication methods. For example, there can be send a message to the administrator's phone or message.

B. Characteristic Matching based on Network Protocol

By way of improving the matching efficiency and adapting high speed network protocol, we use the detect arithmetic based on protocol analysis to analyzing captured data packets. The transmission of user data is based on a curtain or kinds of protocols, for example, in Ethernet system pack the data and encapsulate packet layer by layer, only the encapsulate packet can transmit in curtain protocol. When the packets reached to the destination, system will encode the packets and automatic get the original data. When the data is encapsulated, the protocol will keep back special information. Therefore we can estimate the type of packet by the protocol and match the characteristic of special protocol, then attain better efficiency and reduce calculation. Consequence machine adopt Frete match arithmetic, which assemble Rete net and match factors. Consequence net is composed of four kinds of node, which each node present an item in rule pattern, one or more node connect to form a pattern and create a restrict node in the end to save the fact of pattern matching. The lower part of Rete net is a network of connected node. They connect the patterns of left part , test the variables between the patterns and save the match set of satisfying the conditions. Rule nodes save the name of the rule and PRI. There are collision set in Rete net, which record all the rule of activate. Consequence machine select one of the activation according to the special collision strategy. When the new fact is produced, it will repeat the match of collision and form the consequence step. Symbol information will transform to integer form in the phase of assembly. The match of symbol will soften to compare of integer, which will increase the efficiency of consequence. In order to expand the event of capture, interrupt function is set in the consequence machine. When the new event triggers interrupt, it will start up running "recognizing-action" ring. So the new event will get timely response and satisfy the requirement of real time detection.

C. The Communication Platform

Since the firewalls and the IDSs might not be deployed in the same host. Therefore, there should be providing a

secure communication platform for the cooperating between the firewall and the Intrusion Detection module. In this paper, we employ the SSL protocol to provide a secure application transmission protocol by encrypting the clear text. We employ the OpenSSL to implement SSL protocol. OpenSSL is a free implementation of SSL/TLS based on Eric Young's SSLeay package [9]. OpenSSL requires creating a TCP connection between client and server, and then use the TCP socket to create an SSL socket. The code for a client connecting the server is as the following:

```
Socket sock=tcp_connect(host,port);
ssl=SSL_new(ctx); //Connect the SSL socket */
sbio=BIO_new_socket(sock,BIO_NOCLOSE);
SSL_set_bio(ssl,sbio,sbio);
if(SSL_connect(ssl)<=0)
    berr_exit("SSL connect error");
if(require_server_auth)
    check_cert(ssl,host);
```

Having initiating an SSL connection to a server, then there should check the server's certificate chain. The code for the server is as the following:

```
void check_certificat(ssl,host)
{
    X509 *peer;
    char peer_CN[256];
    if(SSL_get_verify_result(ssl)!=X509_V_OK)
        berr_exit("Certificate doesn't verify");
   peer=SSL_get_peer_certificate(ssl);
    X509_NAME_get_text_by_NID
   (X509_get_subject_name(peer),NID_commonName,
   peer_CN, 256);
    if(strcasecmp(peer_CN,host))
        err_exit("doesn't match host name");
}
```

D. The Communication Platform

In this system, we use the XML as the transmission format. XML is a data interchange format that allows exchange data between different systems or applications. Thus, in this paper, we employ the XML as the transmission unit. For example, if the there is a SYN Flood attack that is detected by the Detection module, then the module calls the Alarm module for notifying the administrator. Also, it generates the instruction report and issue the report to the Policy Handler for further processing. For example, the report can be presented as the following format:

```
<Intrustion_Report>
    <type>SYN_FLOOD<type>
    <protocol>TCP</protocol>
    < src_ip>169.254.94.37</ src_ip>
    < src_port>8080>< src_prot>
    < dst_ip>192.168.10.1< dst_ip>
    < dst_port>80< dst_ port >
    < dst_action>deny< dst_ action t >
    < time>2010-12-14 23:35:59<time>
</Intrustion_Report>
```

Having receiving the instruction report, the Policy Handler adds a rule if the report's action is "deny". For example, if the next request, where host IP address is 169.254.94.37, comes, then the firewalls will block it.

IV. IMPLEMENTATION OF LOAD BALANCE

The implement of diffluent is to maintain a assignment table, which using HASH table to realize access to table. Every unit in the table include <sip, sp, dip, dp，n，rt>, that is: Source IP address, source port, destination IP address, destination port, analyzer host no, update time. In the application of TCP, SYN symbol is to build a new connection, while FIN and RST is to end a connection. When the creation of a connection, it will assign a analyzer to it by load balance arithmetic. Then all the packet of the same application connection will send to the analyzer host. After the connection is ending, the connection record will delete in HASH in order to the HASH overflow. For connectionless UDP application and half-baked TCP connection, it will use update time to clear timeout connection timely.

If the load of each analyzer host is Li (i = 1,2,…n)，0 ≤Li≤100。Ci (i = 1,2,….n) is the ability of analyzer host, which is the application set of support.

Ri (i = 1,2,….n) is the usability, which can be 0 or 1, 1 represent the host can be used. The difference arithmetic based on least load first is describe as follows:

(1) Receive-a-packet(*P*); app-session-id = <*P*.sip, .sp, P.dip, P.dp, P.n, P.rt>; flag = P.tcp.flag
(2) If(flag = SYN) goto (4)
(3) *m* = Hash(app-session-id); Send-packet-to(*P*, *m*); Reset-time-record(); goto(5)
(4) *m* = Find-a-analysis-host() & (R_m = 1) & (P.dp∈C_m) & (L_m=MIN(L_i))
(5) Insert-into-table(app-session-id,m, Get-time-now()); Send-packet-to(*P*, *m*)
(6) If(flag = RST | flag = FIN | IsTimeOut) Delete-from-table(app-seesion-id)
(7) goto (1)

V. Performance Analysis

The system is composed of sensor, analyzer, manager, Intrusion Detection Agent System (IDA) and user interface [12]. In the data flow the output of the former is the input of next components while in the control flow the latter control the former component by relative protocol.

(1) Independency and collaboration.

Intrusion Detection Agent System (IDA) is an independent program. It can be develop and test respectively. Though each IDA is an aspect of host or network, IDA can exchange information to make accurate result.

(2) Agility and flexibility.

IDA can start, stop and dynamic configure respectively. It only need to reconfigure or add IDA if it has new data or new type intrusion.

(3) No limit to data source and small error diffusion.

Different IDA can use different data source. As IDA is realized independently, data source can use kinds of forms, such as: audit data, system configure check, network packet capture etc. If some IDA have problems or been destroyed, only those connected to the IDA will invalidation, IDA will find the state and deal with them. That will limit the harm to the least area.

(4) Platform independent and compatibility

As IDAs are independent, they can be developed respectively. They can also use different languages and base on different platform. They only need to keep to uniform communication protocols and format. The model either include IDA based host, or based network, which exceed the bound of traditional IDS model.

VI. Conclusions

Since the traditional firewalls only analyze the packet's header not the content so that they can not provide dynamic defense against hacker attacks. For addressing these issues, we, in this paper, propose the enhanced firewalls integrating with the intrusion detection technologies. The system can real-time monitors the data packet and modify the security policies. However, it is very likely to generate conflicting rules when adding or modifying a rule. Thus, the enhanced system should provide the function to checks and remove firewall anomalies anatomically to achieve good performance, which will be the next work in our research.

Acknowledgment

This paper is sponsored by the Foundation of Jiangxi Educational Committee (GJJ10478), Project supported by the Key Laboratory for Computer Information Processing Technology, Jiangsu Provincial, China (2008-03).

References

[1] ITsecurity.com. "History of the Firewall" (March, 26, 2011).

[2] M. Nacht. "The Spectrum of Modern Firewalls". Computers and Security, 17(1):54–56, 1997.

[3] http://www.itsecurity.com/dictionary/dictionary.htm (March, 26, 2011).

[4] S. Ehlert,D. Geneiatakis,T. Magedanz, et al. "Survey of network security systems to counter SIP-based denial-of-service attacks". Computers & Security, 29(2):225-243, 2010.

[5] B. Reynolds,D. Ghosal. "Secure IP Telephony using Multi-layered Protection". Proceedings of the ISOC Symposium on Network and Distributed Systems Security (NDSS). 2003.

[6] Yu Fei, Zhu Miao-liang, Chen Yu-feng, et al. An Intrusion Alarming System Based on Self-Similarity of Network Traffic. Wuhan University Journal of Natural Sciences, 10(1) :169-173,2005.

[7] Dayong Ye,Quan Bai,Minjie Zhang, et al. "P2P Distributed Intrusion Detections by Using Mobile Agents". Proc. of the Seventh IEEE/ACIS International Conference on Computer and Information Science, IEEE Press,2008:259-265.

[8] Hamed, H. ; Boutaba, R. ; Hasan, M, et al. "Conflict classification and analysis of distributed firewall policies" IEEE Journal on Selected Areas in Communications,23(10):2069-2084, 2005.

[9] Ping Yi,Xinghao Jiang, Yue Wu, et al. "Distributed intrusion detection for mobile ad hoc networks", Journal of Systems Engineering and Electronics,19(4): 851-859,2008.

[10] E. Al-Shar and H. Hemed. "Firewall Policy Advisor for Anomaly Detection and Rule Editing." Proc. of IEEE/IFIP Integrated Management Conference (IM'2003), March 2003:17-30.

[11] http://www.openssl.org(March, 26, 2011).

[12] Cheng Xu, Fei Yu, Zhenghui Dai , et al. "Data Distribution Algorithm of High-Speed Intrusion Detection system Based on Network Processor". Proc. of the Second International Conference on Semantics, Knowledge, and Grid , IEEE Press,2006:27-31.