DISTRIBUTED FIREWALL DESIGN CONCEPT BASED ON LAN

Ch.Srinivasa Rao[1], Dr. Boddi Reddy Rama[2], D.Pavan Kumar[3]

[1]Research scholar, Rayalaseema University, Kurnool, A.P, INDIA

[2]Department of informatics,Kakatiya university, Warangal, A.P, INDIA

[3]Asso.Professor Dept of CSE, Mother Teresa Institute of Science & Technology, Sathupalli, Khammam A.P ,INDIA

ABSTRACT

Although the theory of distributed firewall was proposed shortly, but because of its advantages relative to traditional firewall, business user oriented characteristics, it could meet customer demand for higher security. This paper proposed a firewall program suitable for network security in accordance with small and medium enterprise network security situation, systematically analyzed the distributed firewall policy management and policy actuator functions, features and related technologies, to discuss the overall design and structure of the log servermodule.

Keywords- *LAN; distributed firewall; policy management; policy actuator*

INTRODUCTION

As a secure means, the firewall is commonly used in the network. Traditional firewalls are not the end-users of the information, cannot test the encrypted data for the absence of information decryption key, so it is difficult to resist attacks on the tunnel. The emergence of a personal firewall makes up some of the shortcomings of traditional firewalls, which more knows the context relationship between the host sessions, while increases a security barrier for the network, but it still cannot fundamentally resolve the internal network security issues. This paper designs distributed firewall architecture suitable for small network.

FIRE WALL ARCHITECTURE

Because small network topology structure is simple, and there is a remote endpoint host, so this paper uses hybrid distributed firewall architecture. For the hosts within the LAN it is much like a traditional firewall, but its security policy is constituted unified by the Center, and then distributed to the internal endpoint host, which needs to use IP address to identify the host status. For remote endpoint host, it first uses certificate to confirm the host identity, and then uses the host IP address and MAC address to commonly identify the host.

The whole distributed firewall system is composed by four main parts: the management center, policy actuator, remote endpoint connectors, and log server. 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. 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. The remote endpoint connectors are the programs specifically designed for the remote endpoint host, to prove their identity to other hosts on a small network, especially the internal endpoint, request to establish communication with the internalendpoint.

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. 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. The whole system architecture as shown in figure 1, to apply the architecture in practical small mixed network should be like this: the management center can be installed on a random host in the LAN, of course, can also be a gateway or other server, but in order to guarantee the security of information, it is best not to install on the gateway host. Local endpoint (including the gateway host) and the remote endpoint all should install the policy actuator, which will run according to the security policy the management center issued to protect all endpoints host security. In the remote endpoints the remote endpoint connector must be installed to connect with the gateway or other internal endpoints, to obtain a higher access privilege than general host in Internet.

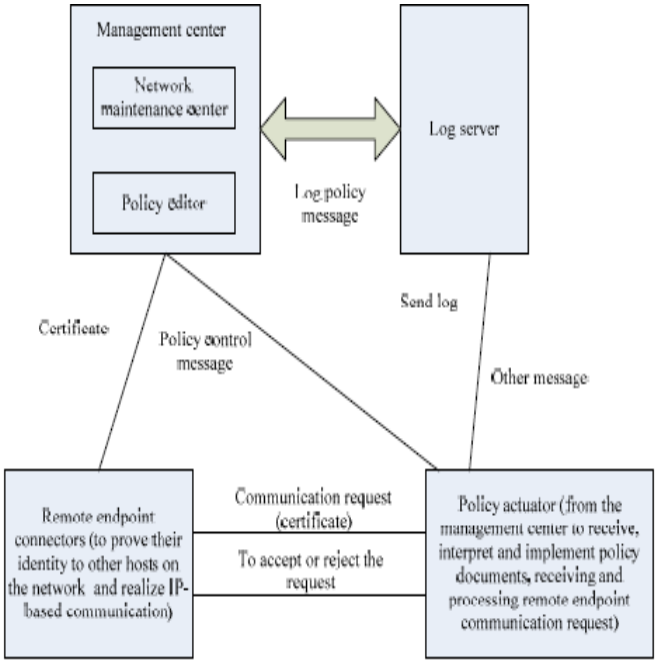

Figure 1. Distributed firewall architecture

LOG SERVER

The log server in the distributed firewall is to receive, process, store, centralized manage and audit the entire internal network, including all protected hosts, border firewall, policy server and other upload log information, it also can realize the real-time monitoring of the internal network status, and based on this, it can achieve the statistic and detection functions based on log information. The log server audit on the log has the following purposes: 1) Reflect the host (network) state within a period of time.2) Through the comparison between short-term records and long -term log, can find the network trends and anomalies. 3) Track the host (network) current network conditions in time. 4) To preserve the historical record, for later use. 5) To authorize the administrator authentication, identification.

Log server task description

Log server functions include three aspects, one is the collection, classification, storage of the information in the system, the other is information processing, recording and display, and the third is the statistical test based on log information. Therefore, when the various functional modules generating log information, they need to write the information into the database through the log server, and carry out statistical analysis through the analysis engine. When the manager required displaying the statistical information, the information should be taken out for analysis to

extract valuable information, provide audit interface, which requests the user interface intuitive and easy querying.

Log server overall structure

Based on the above analysis and consideration, the system's basic operation mode is Client/Server structure, the overall framework as shown in figure 2. SSL encryptedtransmission

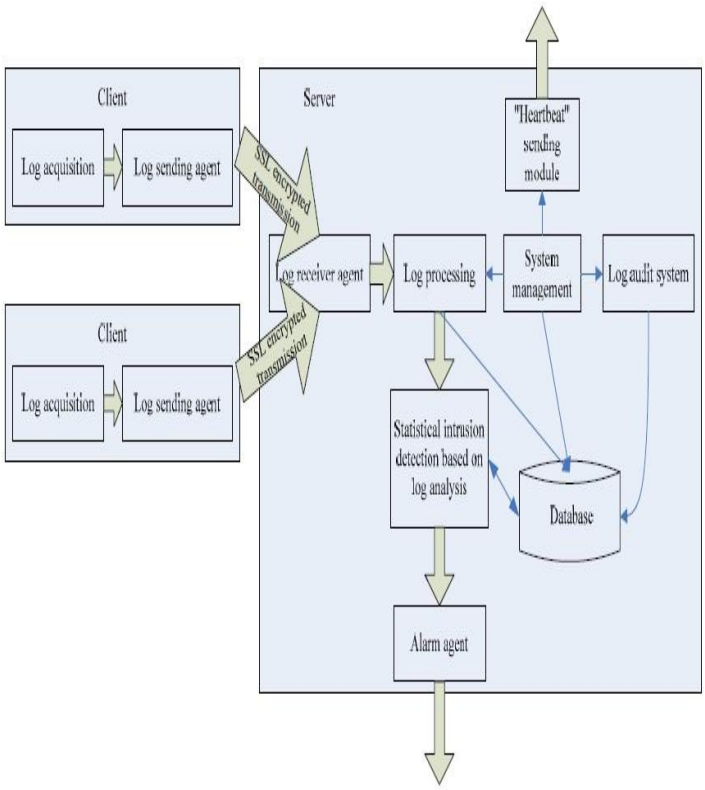

Figure 2. Log server overall structure

The system client refers to the various hosts within the network need to audit, and the sending agents installed on the client are to collect the original logs, this part will be completed by the corresponding host firewall, border firewalls, and policy center, to convert and transfer to the server through SSL encryption. The server is mainly composed by three parts: data acquisition, audit system and statistical intrusion detection based on log analysis. Data acquisition is used to receive the data from the client and store it in the database after processing; audit system is used to coordinate the work of other parts and receive the administrator's configuration adjustment information; statistical intrusion detection based on log analysis is to complete the intrusion detection function and achieve the linkage with other modules. The task of this paper is to design

a multi-client, multitasking software system which runs in Linux operating system environment and is able to complete the abovementioned functional requirements.

POLICY DOCUMENT

The content of policy document not only includes of filter rules, but it also includes of other information, such as certificates, policy file version, management control center and some conventions between the point and the host. They cannot be displayed in the policy editor. Its function is to realize communication between policy implementation and the management control center, and center-to-end for remote management. Packet filtering rules stored in the management and control rules file. It Volume 4 519 can be divided into the following paragraphs according to the stored contents. It is shown as figure3.

File head Time record store IP address range record store Application rule record store Website rule record store ICMP rule record store

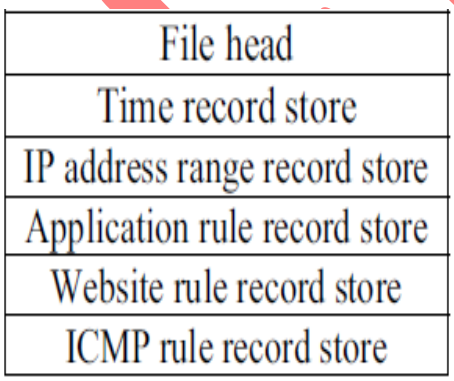

Figure 3. File structure of control rules

There should be a protocol between policy documents and policy actuator, so that the actuator can translate the policy file and execute it. The custom protocol is used in this paper, so the user cannot modify the policy file. If the policy file is changed not according to the protocol, the policy actuator cannot understand and implement a policy file. In order to avoid this case happening, the policy file cannot be saved and transmitted with ASCII plaintext. Its format needs to be changed and became to the format which users cannot be read. So the protocol between policy documents and policy actuator should be added decryption protocol.

POLICY ACTUATOR

Policy actuator is installed on the endpoint host, and 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 functionofthetraditionalfirewall.Additionally,itisalsotoachievethefunctionsof

communicating with the management control center and establishing communication link request for the remote endpoint. The packet filtering technology is chosen to achieve the function of Policy actuator for the following considerations.

Packet filter

The head information of outgoing data packet will be filtered according to the policy file rules, and it will decide how to deal with the package. Packet filter rule is a chainlike structure. The data packet and the first rule will be compared. If it meets the rule, the package will be handled under the rules (discarded, to allow, modify header information, etc.). Otherwise, the package will be compared with next rule. If there is not a matched rule when it reached at the end of the chain rule, the default policy of rule chain will be implemented. The three built-in rule chains: INPUT, OUTPUT, and FORWARD will be defined according to the data packet transmission direction and its state. The Packet filter program will find the corresponding rules chain to match according to packet transmission directions. Users can define their own chains for easy to manage, but it is only included in the built-in chain. It is just a collection of some of the rules and it has not defaultpolicy.

Log filter

The log is notes of packet header information which meet certain conditions according to the rules. Users can know the situation of the firewall running and discover some problem by analyzing the log. As the log file is saved as the user readable form, the user can directly view the log file, or use the log analyzer to view. The path of the log file can be specified. Users can prescribe the log level and log prefix except the record head information for easy to classification view when writing the log. The log prefix is entirely defined by users for easily to understand the stringmeaning.

State inspection

As known, TCP connection is established through the three-way handshake process. The process of connection establishment and closure can be described by the exchanged data packets states. A packet can have the following states: New: a new packet which has been established. ESTABLISHED: an already exists packet which belongs to the connection packet. RELATED: a packet which is related with the current connection, but it is not belonged to the current connection, such as ICMP error packets or the established FTP connections. NVALID: a package which cannot be recognized for some reason. The reason is included of memory deficiency and ICMP error which cannot be responded to any connection. These packets can be discarded at usually. Users can write the filter rules according to the state which is confirmed by the policy editor program through tracking the connectioninformation.

Intrusion prevention

The purpose of intrusion prevention is to prevent the common means of attack by users' simple setting, such as IP deception, attacks on application-layer protocol vulnerabilities, DDoS, and so on. It is embodied in the aspect of discarding the package which source address or destination address is unreasonable, discarding the package which is connected to the specific port, limiting the packet quantity which is met to certain conditions in certain period, and so on.

Communication with management control center

Policy editor should frequently communicate with the management control center. Here the method of setting a specific port in the endpoint host and the port is set as 8899. When the management control center connects with the port 8899 of endpoint host, it should send its own key to the endpoint. The communication will be beginning after the identity has been confirmed. Otherwise, the endpoint will close the connection. The connection which is sent by endpoint will be processed with the same manner. The communication content which is between control center and endpoint includes as follow.

1) The policy document which is released by the center and sent to thehost.
2) The policy document which is required by the host and sent to thecenter.
3) The policy document edition which is asked by the center and sent to thehost.
4) The policy document which is required by the center and sent to thehost.
5) The control command which is issued by center and sent to the host. Clearly, the detail interface which is between the control center and policy editor is needed to bedefined.

REMOTE ENDPOINT CONNECTOR

As the remote endpoint is located outside the LAN, so how to distribute them from other hosts in the internet is the main problem which should be solved firstly in the distributed firewall system. As using the traditional IP address to identify the host identity is very reliable and the host has not a fixed IP address in the dial-up internet, here the certificate will be used to identify the identity of the remote endpointhost.

Each remote endpoint will be assigned a certificate, when it needs to communicate with the server on the LAN, it should first send its certificate to the server to prove its identity. The program to complete this function is called as remote endpoint connector. Remote endpoint connector establishes TCP connection with the control port of the server policy actuator, sends its own certificate to the port of the server, and after the server authenticating the certificate it will add the rule in its own firewall rules to allow the communication with the host, and then sendconfirmationmessagetoaconnector,whichexpressesthecommunicationhasbeen

allowed. In this state, the remote endpoint can communicate with the server on the LAN. After communication, the user should close the connector or command the connector to inform server that the communication has been ended. If the user does not carry out this operation, the server will interrupt the communication (remove the rules allowed communication from the policy) after a certain time of no data packet exchange between the two, and notify the connector that the channel has beendisconnected.

CONCLUSION

This paper designed a distributed firewall system suitable for small network based on the actual situation of current network in China, analyzed the three parts of it, which are management and control center, policy actuator and remote endpoint connector. And finally the specific functions of them were analyzed in detail.

REFERENCES

[1] Lowe.G.,AnattackontheNeedhan-SchroederpublickeyauthenticationProtocol[J], Information Processing Letters, 1995, 56 (3):131-136

[2] Jablon.D., Strong password-only authenticated key exchange [J], ACM Computer Communication Review 1996 26 (5):5-20

[3] Housley.R., Internet X.509 Public Key Infrastructure Certificate and CRL Profile[J], Network Working Group, 2002, 54-62

[4] DavidKormann.P,AvielRubin.D,RisksofthePassportsinglesignonprotocol[J], Computer Networks, 2000, 33:51-58

[5] Bellare.M, Pointcheval.D, Rogaway.P, Authenticated key exchange secure Against dictionary attacks [J], In Eurocrypt, 2000, 18(1): 139- 155 Volume4