Volume 1, No. 4, Nov-Dec 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

"Usage of Firewall Technology in Web Application Security"

Kamlesh Malpani
Lecturer, Shri Vaishnav Institute of Management, Indore (M.P.),India
Malpani_k1@rediffmail.com,No.9425477438)

ABSTRACT: At present, the firewall has become the world's most widely used network security products. Firewall technology as secure e-commerce activities, information security, the first effective barrier by more and more attention. In the Internet network and an internal network set up between the barriers and prevent hacker access to the internal network, secure access by users to develop strategies to resist a variety of invasive isolation techniques. Especially for today's largest networks - the Internet, are vulnerable to malicious attacks people with ulterior motives and destruction. In this paper, firewall concepts and techniques starting a detailed analysis of the firewall functionality and to ensure the safety of their different methods of research were classified. With the continuous development of e-commerce, network security firewall technology will play more important aspects of the role and value.
Keywords: Network Security, E-commerce, Packet filtering.

I. INTRODUCTION

In the information society, information has and energy, material source of equal value, in some cases even higher value. Valuable information on security issues are bound to exist, especially for businesses. Economic and social development also requires communication between the various users and resource sharing needs to be a group of computers connected into a network to ensure the normal conduct of e-commerce activities, thus bringing more security risks. Especially for today's largest networks - the Internet, are vulnerable to malicious attacks people with ulterior motives and destruction. Disclosure of information has become increasingly serious problem; therefore, computer network security issues become increasingly important.

How to ensure the security of computer networks as well? Although many methods, but the firewall technology is definitely one of the most efficient and practical methods. In building a secure network environment in the process of a firewall as a first line of defense, is being more and more users attention. Usually a company to buy network security equipment, always give priority to the firewall. At present, the firewall has become the world's most widely used network security products. So, the firewall is how to ensure the security of network systems, but also how to achieve their own safe? In this paper, the firewall concept, a detailed analysis of the firewall functionality, in accordance with its guarantee of the different security methods have been classified: packet filtering firewall, service proxy firewall, the address migrating firewall.

A. Firewall Introduction

Firewall is a kind of internal networks and public access networks separate method is a special kind of access between the network control facilities. In the Internet network and an internal network set up between the barriers and prevent hacker access to the internal network, secure access by users to develop strategies to resist a variety of invasive isolation techniques. It allows you to "agree" to enter your network and the data will be "no consent" and the data in the door to maximize the network to prevent hackers to access your network and prevent them from change, copy, destruction of your important information; to limit the protected network and Internet networks, or with other networks of information between the access, transfer operations; according to corporate security policy control access to network information flow, and itself has a more strong anti-attack capability. Is to provide information security services, achieve network and information security infrastructure. Logically, a firewall is a separator, a limiter, but also a parser to effectively monitor the internal network and the Internet between any activity to ensure that the internal network security. Firewall security technologies, including packet filtering technology, agent technology and address of the migration technology.

II. THE ROLE OF FIRE WALL

A. As A Network Security Barrier

Only carefully selected application protocol to pass a firewall, enable the network environment has become more secure. NFS protocol, such as firewalls can prohibit access to a protected network, so that outside attackers can not take advantage of these fragile agreement to attack the internal network. Firewalls also can protect the network from routing-based attacks, such as the IP source routing options in the attacks and ICMP Redirect in the redirection path. The firewall should be able to reject all of the above types of attack packets and inform the firewall administrator. A firewall is a term used for a ``barrier'' between a network of machines and users that operate under a common security policy and generally trust each other, and the outside world. In recent years, firewalls have become enormously popular on the Internet.

B. Can Strengthen The Network Security Policy

Through the firewall-centric security solution configuration, can all security software (such as passwords, encryption, authentication, auditing, etc.) configured on the firewall. And network security issues distributed to each host, compared to the firewall and centralized security management more economical. For example, network access, the one-time pad system passwords and other

identity authentication system can not scattered in various hosts, and concentrate on the firewall body.

C. Can Monitor And Control Network Access And Access To Audit

If all access is through the firewall, then the firewall will be able to record and make the log records of these visits, but also be able to provide network usage statistics. When a suspicious action, the firewall can make the appropriate alarm, and to provide the network is being monitored and attack details. In addition, the collection of a network use and misuse of the situation is very important. It is clear whether the firewall can fend off the attacker's detection and attack, and a clear control of the adequacy of the firewall. The network usage statistics on the network needs analysis and threat analysis, is also very important.

D. Can Prevent Leaks Of Internal Information

Through the use of a firewall into the internal network can be realized within the network focus on network segment isolation, thus limiting the local network security key or sensitive issues on the impact of the global network.

E. Other Role

A. The primay role of a firewall in an intranet (versus internet) is to enforce security policies between different branches/offices/departments within the company.
B. Firewall compromise would be potentially disastrous to subnet security. For this reason, agencies will, as far as is practical, adhere to the below listed stipulations when configuring and using firewalls.
C. Limit firewall accounts to only those absolutely necessary, such as the administrator. If practical, disable network logins.
D. Use smartcard or authentication tokens to provide a much higher degree of security than that provided by simple passwords. Challenge-response and one-time password cards are easily integrated with most popular systems.
E. Remove compilers, editors, and other program development tools from the firewall system(s) that could enable a cracker to install Trojan horse software or backdoors.
F. Do not run any vulnerable protocols on the firewall such as TFTP, NIS, NFS, UUCP.
G. Consider disabling finger command. The finger command can be used to leak valuable user information.
H. Consider not using the e-mail gateway commands (EXPN and VFRY) which can be used by crackers to probe for user addresses.
I. Do not permit loopholes in firewall systems to allow friendly systems or users special entrance access. The firewall should not view any attempt to gain access to the computers behind the firewall as friendly.
J. Disable any feature of the firewall that is not needed, including other network access, user shells, applications, and so forth.
K. Turn on full-logging at the firewall and read the logs weekly at a minimum.

III. THE FIREWALL'S TECHNICAL CATEGORIES

A. Packet Filtering Technology (Packet Filter) Firewall

Packet filtering is a network layer packets through the implementation of a choice, based on the system pre-configured filtering logic, and check the data stream according to each packet, according to the packet source address, destination address, and the package used by port to determine whether to allow such packets. Information on the Internet such a packet-switched network, all incoming and outgoing information is divided into many a certain length packets, packet includes the sender's IP address and IP address of the recipient. When these packets are sent to the Internet, the router reads the receiver IP and select a physical line to send out information packets may arrive in a different route destination, when all the packets arriving at the destination after re-assembled to restore. Packet filter firewall to inspect all through the bag's IP address and the system administrator in accordance with the given filter information packet filtering rules. If the firewall configuration an IP as dangerous, then, from this address from the firewall all the information will be masked.

Packet filtering router, the biggest advantage is that it is transparent to the user, i.e. does not require a user name and password to log on. Such a firewall fast and easy to maintain, usually as the first line of defense. Packet filtering router is also very obvious shortcomings, usually it does not have the user's records, so as not to access records from hackers records found. To attack a simple packet filter firewall to the hacker is relatively easy. Such as "packet shock" is a hacker as a means of attack the more common, hackers on the packet filtering firewall issued a series of packets, but these packages in the IP address has been replaced, and replaced by a string of sequential IP Address. Once a packet through a firewall, hackers can use this IP address to disguise their messages. Usually it does not have the user's records, so that we can not access records from hacker attacks found record; In addition, the configuration is complicated as a packet filtering firewall shortcomings. It blocked entry to the internal network, but it does not tell you what to enter your system, or who access the Internet from within. It prevents outside of private network access, but not recorded within the visit. Another key weakness of packet filtering is not on the user level filtering, that can not identify different users and to prevent theft ip address. So the packet filter-based firewall is a sense of security systems.

B. Firewall Proxy Service

Proxy service is another type of firewall, which is usually a software module, running on a single host. Co-operation with the router, proxy server, router, internal and external networks to achieve the flow of information interact-oriented, all the relevant application service requests passed to the proxy server. The role of agency services at the application layer, which is characterized by completely "barrier" of the network traffic flow for each application service through the establishment of a special agent to achieve monitoring and control application-layer traffic role. The essence of agency services intermediary role, it does not allow the internal network and external networks for direct communication between the user.

Users want to access the intranet, when an application server is actually running on the firewall to the proxy service software request, to establish a connection; reason to access the server on behalf of its applications to the request to establish a connection; applications for a proxy server response; proxy server for external network users in response to. Extranet users and application server data transfer between the transit entirely by the proxy server, external network users can not interact directly with the application server to avoid attacks from outside users. Proxy service is usually application-specific services, and different applications can be set to a different proxy server. At present, many of their internal networks using both packet filtering routers and proxy servers to ensure the security of internal network, and achieved good results.

C. Address To Migrate Firewall

A variety of reasons, IPv4 address depletion crisis facing the gradual, but take some time before the practical application of Ipv6. With the growing number of online businesses, businesses to obtain a public IP address (called the global IP address, or the actual IP address) and business Internet access may be difficult to match the number of actual devices, this phenomenon has a tendency to increase. One possible solution is for each firm a number of global IP addresses assigned, enterprise networks for internal use custom IP address (known as the local IP address or virtual IP address). When the internal and external user wants to visit with each other, specialized router (NAT router) is responsible for the global / local IP address mapping. NAT router addresses in different domains of the border, by retaining part of the global allocation of IP addresses to support IP datagram the right to inter-network transmission. The working principle: (1) address binding (static or dynamic establishment of local / global address mapping); (2) address lookup and translation (data reported in the relevant address information be modified); (3) Address Solution bind (released the global address).

Address migration actually combines firewall packet filtering and application proxy design ideas, can be limited depending on the application needs to allow internal and external network access node; can shield the address within the network to ensure that intranet security. Packet analysis is a NAT router must be done (for example, modify the IP datagram carrying a high-level protocol data unit, the address information), so you can selectively provide / refusing some of the inter-network applications.

IV. SUMMARY

On the Internet firewall is a very effective network security model, risk areas can be isolated through its regional connectivity and security while not compromising people's access to risk areas. With the continuous development of e-commerce, network security firewall technology will play a more important aspects of the role and value. Security is a difficult job that involves constant care. Computer systems or other networked devices are vulnerable by virtue of their ability to connect and communicate with other systems. A firewall reduces some of the risk by reducing the number of devices that can communicate with a protected host.

V. REFERENCES

[1] peak Xu Shan: firewall packet filtering rules of the study [J]. Applications, 2003,23 (6)

[2] Zhao Qibin Liang Jing Zhang: firewall filtering rules anomalies research [J]. Engineering, 2005.12

[3] Xie Xiren: Computer Network Technology [M]. Beijing: Electronic Industry Press, 1999

[4] http://en.wikipedia.org/wiki/Firewall_(computing)

[5] http://www.experts-exchange.com/Security/Software_ Firewalls/Q_21335372.html

[6] http://www.it.northwestern.edu/bin/docs/firewall_ strategies_wp.pdf