Research on Computer Security and Firewall Technology

Ping Chen [1]

[1] College of mathematics and computer science, Jiangxi Science and Technology Normal University, Nanchang, Jiangxi , 330013

KEYWORDS: Computer Security, Firewall Technology, Analysis, Application

ABSTRACT: In this paper, computer security and firewall technology for a simple analysis, and then study the type of firewall technology, principles and the latest firewall technology, and to make some research on the firewall technology in computer security, such as the configuration of security services, configuration access the strategies.

Introduction

With the rapid development of science and technology, the network gradually integrated into our lives, study and work, has brought great changes, while people over computer networks faster exchange of information, sharing and communication. However, in the computer network, because there are information technology reform and innovation space, development is not perfect, there are some computer network security issues, to bring a lot of trouble. If you do not solve these problems, it will greatly hinder the development of computer networks.

The Meaning of Computer Security and Firewall Technology

Computer network security to some extent refers to the network information security, data in a computer network cannot be subject to some malicious destruction or accidental disclosure, alteration, etc., enabling continuous normal work network, and network information services will not interrupt. For network information can be done integrity, confidentiality, authenticity and controllability.

Firewall technology is a kind of isolation between the network and the network side of the security barrier set up to ensure the network and information security. Firewall technology can not only network information technology properly controlled, can resist outside attacks, thus preventing other users illegal access to relevant network information resources. For the protection of internal security apparatus also has a role.

Factors that Affect the Computer Network Security

There are many factors that affect computer’s network security and they are divided into subjective factors and objective factors. Subjective factors generally include man-made malicious attacks, sneak into someone else's computer to find loopholes in the system, the use of non-normal means to steal or destroy data, there are various systems virus, some network resource abuse, loopholes in management, information leaks, etc. Objective factors including the impact of some of the harsh environment, aging equipment, electromagnetic interference and so on computer network security caused a certain degree of threat. Most major factors are the following:

First, information is disclosure and tampering. This refers to the network to upload information from eavesdropping, but does not destroy the network to transmit information. Information has been tampered with is not only refers to the intruder eavesdropping network information, but also made some changes to the information, making information about its authenticity, played a role in misleading information.

Second, there are vulnerabilities of operating system. This is a major threat to network security threats. Since the existence of the computer operation complexity makes network services and network protocols cannot effectively achieve, so in a complex implementation process, resulting in the computer operating system, there are some loopholes and defects.

There is network information openness under the resources sharing. Due to the openness of the network and other information, civilians or government sensitive information is available on the computer network, thus giving criminals can take advantage of the machine, the network elements to provide more detailed information to facilitate their criminal behavior.

Fourth, there are software vulnerabilities. Software vulnerabilities typically include operating systems, network software and services, application software, database, TCP / IP and other vulnerabilities. There are vulnerabilities so that if the computer has a virus attack, it will cause a great threat to network security.

Type of Firewall Technology

Proxy firewall technology is generally divided into a firewall, packet filtering firewall and detection type of firewall. Proxy firewall is a proxy server, high safety factor, technology is more advanced. In today's proxy-based firewall technology is more comprehensive in the development and application of computer networks. Proxy Firewall is usually used as a transit point information data between users and between. Which can effectively resist some of the hazard information, his wife work at the OSI highest level, with full "barrier" characteristics of the network traffic, and is designed for the preparation of the agent application services, it is possible to effectively monitor and control the implementation of the action.

Packet filtering firewall technology is more of the old, the key technology is the sub-transmission network information, different packets represent different meanings, firewall technology these packets is judged safe or not, the command to allow or block. This type of firewall technology has the ability to adapt to the environment is relatively strong, low cost, convenient and simple, practical, good advantages. But there are also disadvantages to the target, or source port of the packet is determined whether to release, whether it is safe range may make malicious programs or data information has not been recognized, resulting in information security threats. Such as e-mail viruses, Java programs carry viruses.

Detection type of firewall is the real-time monitoring information for the data, and automatically detected. Which to some extent it can effectively improve the security features of your computer. But this firewall technology there are some disadvantages, such as the inconvenience management, higher costs. Thus this detection type of firewall technology has not been widely applied to the implementation of computer network security.

Principles of Firewall Technology

In the first type of firewall technology classification, proxy type of firewall technology works by providing proxy support at the application level. For example the FIP, SNMP, HTTP, TELNET and so on. The so-called proxy service is confirming the connection request from the client effectively

take over the connection, and then issue a connection request to the target server, according to the response of the target server, the appropriate decision as to how the client requests.

Proxy Server should generally connection and proxy server processes, process and agency services connecting clients. Acting at the same process should also be extended to maintain a collection of fields, providing authorization and authentication. Such as allowing FIP command is to prevent certain files through the firewall, file type support FIP security filtering.

Firewall technology commonly used in the classification of the second type, packet filtering firewall technology. It works through the firewall packet contents set by the user or custom rule set specific firewall software. Such techniques should allow experienced network operators to gather information on the latest attack, in order to analyze data loaded name, direction, type, protocol, description, TCP flags and data chain. Meanwhile packet filtering firewall technology should include all methods of access to the firewall packet processing, with some detection mechanism to prevent data collisions. Such as IP packet filter mainly relies on the source site IP packet header or IP address of the destination station IP for data filtering. There are other MAC address filtering, application-based RPC service filtering and FIP filter and so on.

The latest firewall technology design goal is a comprehensive application proxy technology and packet filtering technology, in order to correct these two technologies in computer network security aspects of the problems.

The Applications of Firewall Technology for Computer Security

The Cluster Systems Management Server, and carved out a separate security service called Quarantine. Security Services division makes a good quarantine is not only an independent regional network, is an integral part of the internal network. In some ways, it helps to ensure system management are protected, while allowing the data on the server in a safe state. At the same time, it can also be transformed firewall technology to achieve network address of the internal network protection. Can all host address to be set to achieve effective network IP address, and network address set to public. This shield external IP address has an important role, not only can effectively protect the safe operation of the computer network, but also can effectively protect the computer network IP address. The use of packet filtering firewall technology can effectively reduce the cost of the firewall, while protecting network security.

The so-called configure access policy, refers to the core of a general firewall security policy. Therefore there must be systems using statistical or detailed information note. At the same time during the setup process should also be the source address setting unit, TCP or UDP port, then this application in accordance with the policy team to configure access to sort, sort of principle is configured and implemented in accordance with the rules of the table position. Configure access policies in accordance with the order of execution, can effectively improve the application firewall technology, while helping to enhance the efficiency of firewall technology when applied. Before receiving data, you need a firewall for certain data validation and testing to ensure the security of information, in order to reduce the risk of computer network security, enhance computer security. Therefore, the computer not only need to have access policy configuration, but also requires the full liberalization of the other integrated application security technology together to increase overall confidence in the safety level.

References

[1] Zhang Rui. computer network security and firewall technology [J]. Computer Knowledge and

Technology, 2012,24: 5787-5788.

[2] Wang Liling. Talking about computer security and firewall technology [J]. Computer Development & Applications, 2012,11: 67-69.