Discussion on Several Typical Computer Network Security Technologies in China

Liangying Chen
Sichuan Vocational College of Information Technology, Guangyuan 628017, China

Keywords: Firewall technology; Virus protection technology; Virtual private network technology.

Abstract. The application and development of computer technology have driven and promoted the change of information technology. The computer and information technology have a wide range of penetration and affinity, which influences the world economy and social development in all aspects. In twenty-first Century, the human life will be more closely linked to the Internet, and more closely related, such as electronic commerce, information platform, etc. However, all kinds of problems arise, for example, there are many threats and attacks existing in the Internet, making the network security damaged, which can cause the disclosure of information, and the system platform and the network resources are under attack. In consequence, in terms of how to ensure the information is sent and received truly, completely, effectively and legally, the issue of network security has become a current research hot-spot. This paper, in allusion to this problem, introduces and analyzes several typical computer network security technologies, including firewall technology, virus protection technology, and virtual private network technology, also called VPN technology.

1. Introduction

Network security is a common concern of people. We can imagine, after several decades, the society will enter a new era of the Internet and the information age. As a result, the importance of network security is outstanding, so mastering more network security technologies is essential. Firewall technology is a very important safeguard for network security. Firewall plays an irreplaceable role in network security protection. The latest generation of firewall technology has a considerable increase, such as encryption anti-virus, technology, multi ports, and security audit and so on, and these functions make the firewall have a more important role [1, 2]. As is known to all, in the process of the development of today's society, the application of computer technology and network technology indeed greatly changes many aspects of our life, and in various fields it has been widely promoted and used. From this point of view, the positive role it plays is more prominent, but with respect to this positive effect, once the computer network is infected by virus, it may cause some large losses, which is more serious in some special industries. In consequence, it is very necessary to study the application of virus protection technology in computer network. VPN technology is the core part of the virtual network, and by the VPN technology, it can realize the sharing and transmission of resources, reducing the investment risk and in the meanwhile creating the enormous use value, to achieve the stability and security of the network environment. In some ways, VPN technology can combine information and users together to ensure that the Internet, in the normal operation, can also hide transferring data in place.

2. Introduction to Typical Computer Network Security Technologies

2.1 Firewall Technology

Firewall is a system with combination of software and hardware, in a dedicated network and shared network, constructing a barrier for the internal network. The main principle of this system is to establish a secure gateway and to achieve protection. For a networked computer, all the data must go through a specific software and hardware equipment, which is a firewall.

For a network, the so-called "firewall" is a specific set of methods and techniques, which can isolate the internal network with the external network. The firewall can establish an access control

between two mutually communicating networks [3-5]. It can realize two functions, one is to isolate people and data that does not conform to the conditions in the external network, the second is to permit people and data conform to the conditions to enter. In other words, the data through the firewall is a necessary condition for the communications of internal network members with the external. Firewall has a very good protective effect that the intruder must first pass through the firewall's security line, so as to contact the target computer.

2.2 Virus Protection Technology

Computer virus refers to let the destructing computer function or data inserted the computer program that is running, when impacting the use self-copy a set of program code or computer instructions. Its intrusion way is divided into three kinds.

Code replaces dumping. The virus mainly uses its own virus code to directly replace an invasion process order module, which is to attack the specific procedures. There is a strong pertinence, which is difficult to eliminate because it is not easy to be found. (2) Source code embedded intrusion. Computer high-level language source code is the main object that the virus invades, namely before compiling the source code, computer virus code is embedded in them. After homologous program is embedded in the virus program, they are compiled executable file together, and the virus file is the invasion results [6].

The current computer viruses often have a variety of features, mainly reflected in the following. It has strong camouflage and reproduction infection. Accompanied by more and more mature computer technology, there are more and more harms to the virus, not just computer programs to be tampered with, at the same time having a certain destruction and change function for computer data and information, and thus seriously threaten the user's computer security. Although there is some computer anti-virus software, there are also some computer viruses disguised to some extent, a relatively strong concealment, which is difficult to be found that it has a certain destructive effect of user information and other documents.

2.3 Virtual Private Network (VPN) Technology

The concept of VPN network technology is to rely on the public switched telephone network (PSTN), to establish a special data file communication channel, and rely on Internet services provider ISP and other network service provider NSP, which uses a tunnel, encryption and other related technologies in order to meet customer requirements for the privacy of documents. Although the VPN is superposed on the public network, it can be regarded as a virtual network, which refers to a logical network. VPN network is isolated from other networks, having good secrecy so as to guarantee the confidentiality when the enterprise is in the transmission of information. At the same time, the electronic information can ensure effectiveness and timeliness of internal information transmission, which will greatly improve the working efficiency of enterprises. Based on the above advantages, VPN network has been widely used and developed rapidly in various large enterprises. With the continuous progress of communication technology, VPN technology has been continuously improved.

3. Design and Realization of Typical Computer Network Security Technologies

3.1 Packets Filtering Firewall

Packets filtering firewall, as a kind of firewall technology, based on the protocol specific standards, the router has the ability to distinguish and restrict in its ports. Its technical principle is that the router added with a filter function to review the information of packets one by one, and in accordance with the rules of the match to decide going forward or discarded, so as to achieve the purpose of refusing to send suspicious packets.

3.1.1 Allocation of Packets Filtering Firewall

The allocation of packets filtering firewall is shown in Table 1.

3.1.2 Realization Content of Packets Filtering Firewall

The major specific realization content of packets filtering firewall is shown as follows.

(1) # ! Bin/bash

(2) iptables-F
(3) iptables -t nat- A POSTROUTING -s 192.168.1.0/24 -o eth0 -j SNAT -to 202.199.24.234
……
(14) iptables -A FORWARD -p icmp -m limit --limit 1/s --limit - burst 10 -j ACCEPT
Example of the steps to build a firewall is shown as Figure 1.

Table 1 The allocation of packets filtering firewall

Items of allocation	Contents
www server	192.168.1.10
ftp server	192.168.1.20
Email server	192.268.1.30
Internal web	192.168.1.0/24
Eth0 (networking with internal web)	192.168.1.1
Eth1 (networking with the Internet)	202.199.37.234

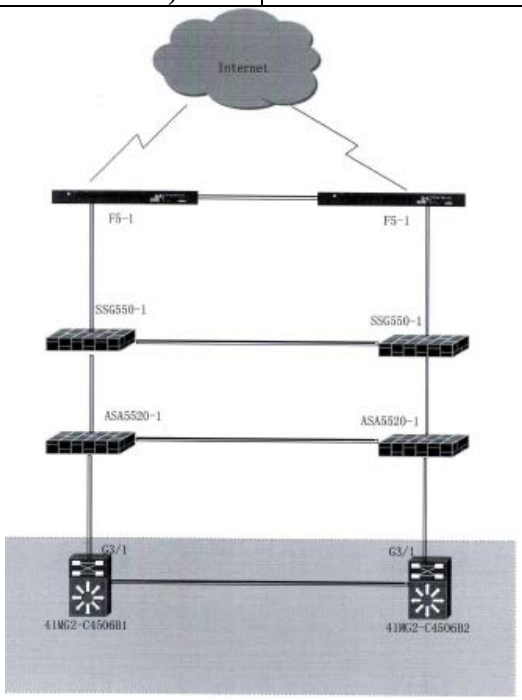

Figure 1 Example of the steps to build a firewall

3.2 Anti-virus Program Design

Our existing network anti-virus software cannot be very effective control of the virus, which is because of the special characteristics of some viruses, and diversity and particularity of the client's server in the actual work. To solve the current problems in network security, it cannot only be done by adding equipment, promoting safety knowledge, and proposing safety requirements, but to establish an anti-virus security system composed of software and hardware and network. The security system we establish have to possess the following functions: security access mechanism, static address binding function, the terminal management function, and the compatible function of existing network environment and anti-virus software.

As shown in Figure 2, access to the network in a transparent way [7]. When all the terminal computers want to access the network, the data packets are required to pass through the gateway of the anti-virus wall equipment. Anti-virus wall equipment at this time can carry out the virus detection and examination required by the terminal computer security requirements.

Design principle: the terminal computer access to the external network, first through the security access mechanism of the anti-virus wall detection. If there is no installation of the client's agent plug-in, it will be forced to install it. The agent plug-in can achieve some of the terminal management functions, mainly to achieve the static address binding function, ARP cheat blocking function, and information feedback function. And then detect whether it is installed the virus software with unified requirements, realized by the agent plug-in information feedback function. If it is not installed, then

turn to the server anti-virus installation interface, automatically install the anti-virus software with unified requirements. The anti-virus software can timely and unified examining and eliminating the virus. And then detect whether it updates the Microsoft patch in time, achieved by the agent plug-in information feedback function. If the patch is not upgraded to the appropriate version, then turn to the server patch installation interface, prompting to download and upgrade the corresponding patch program (Figure 3).

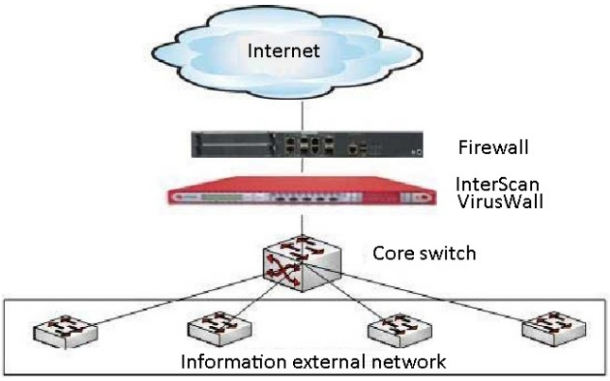

Figure 2 Access to the network

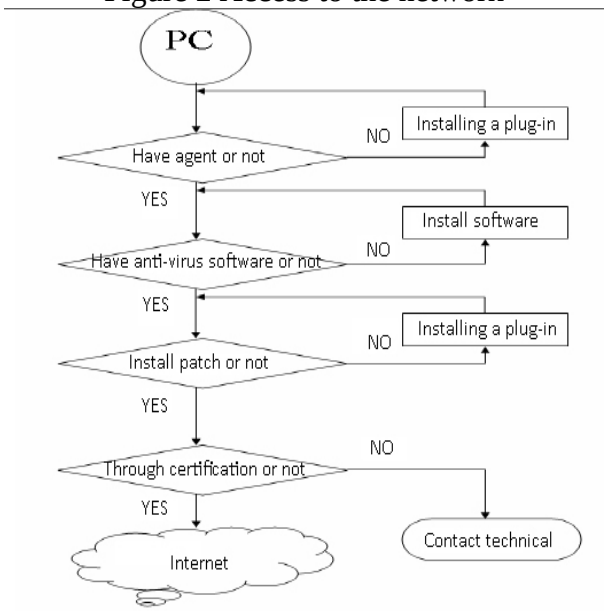

Figure 3 The flow chart of anti-virus wall design

3.3 Design of VPN Technology

The composition of the VPN system can be divided into VPN server and VPN client according to the function. The role VPN server plays is similar to a proxy server, which is a public network access to the private LAN Bridge, and it protects the LAN topology information. The role of VPN client is equivalent to a proxy client. When the application program requires access to the LAN resources, it sends request to the VPN client, the VPN client create a secure channel to VPN server, and then forward the application program and communicate in the LAN. It provides a safe channel for remote computer through the public network access to the private LAN, making the remote computer safely access to the private LAN resources. The overall design is shown in Figure 4 [8].

In order to further improve the VPN communication confidentiality, placing a corporate firewall before the proxy server. If the users expect to securely connect to the corporate network, so when users input a URL, bypassing the firewall in the browser, the connection will be made by the proxy server, and verify the identity of the user, then the proxy server will provide a remote users and connect with a variety of applications server.

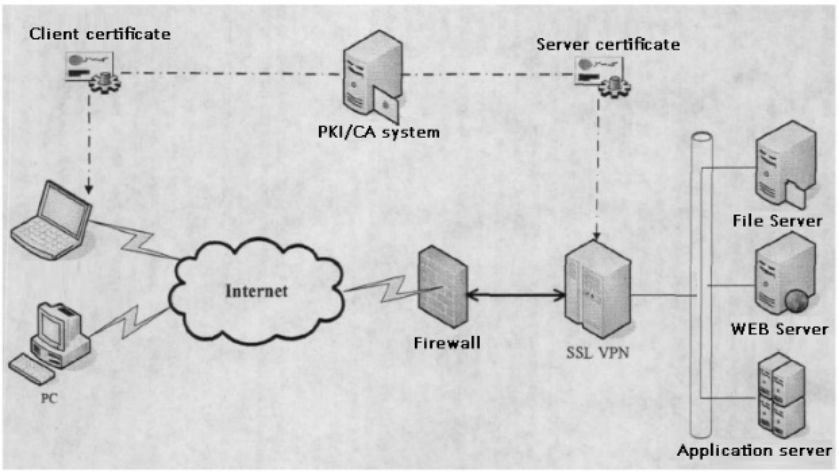

Figure 4 The overall design of VPN technology

4. Conclusion

With the rapid development of economy, the computer technology has more and wider application range. At the same time, with the development of knowledge economy diversification, computer network security has gradually become one of the focus of attention. This paper, through the analysis of the current network security firewall technology, proves that the firewall technology plays an important role in the maintenance of network security. The application of virus protection technology in computer network is based on the purpose of protecting the data of computer information. By taking a scientific and effective prevention and control of virus technology, do security protection of software well, to ensure the security of computer information from the fundamental and ensure the security of computer network. Moreover, from the analysis, we understand that the technical direction of VPN technology is mainly related to the progress and development of new business. Only completely combine technical advantages can the practical effect get to the best. Only by combining the major typical computer network technologies can the network security be better guaranteed.

References

[1] Li J. The research and application of multi-firewall technology in enterprise network security [J]. Int'l J. of Security and Its Applications, 2015, 9 (5): 153-162.

[2] Ling-Fang H. The firewall technology study of network perimeter security[C]//Services Computing Conference (APSCC), 2012 IEEE Asia-Pacific. IEEE, 2012: 410-413.

[3] Shuo L. The specific application of firewall technology in computer network security [J]. Network Security Technology & Application, 2013, 10: 014.

[4] Min C. A Brief Analysis on the Firewall Technology & Network Security [J]. Office Informatization, 2013, 16: 007.

[5] JIANG E, LI S, ZHAO Q, et al. Experiment Teaching Design of Firewall Technology Based on Packet Tracer Software [J]. Journal of Tonghua Normal University, 2013, 8: 019.

[6] Schillie S, Murphy T V, Sawyer M, et al. CDC guidance for evaluating health-care personnel for hepatitis B virus protection and for administering post exposure management[J]. MMWR Recomm Rep, 2013, 62(10): 1-19.

[7] Stewart W M, Carrera M, Hook R G. Computer virus protection: U.S. Patent 8,769,258 [P]. 2014-7-1.

[8] Liu J, Yong W. Application of Multi-Campus Network Based on MPLS VPN [J]. Value Engineering, 2014, 3.