© IJARW | ISSN (O) - 2582-1008
March 2025 | Vol. 6 Issue. 9
www.ijarw.com

DISCUSSION ON THE APPLICATION OF VIRTUAL NETWORK TECHNOLOGY IN COMPUTER NETWORK SECURITY

Dinh Thi Kim Ngoc[1], Pham Hong Truong [2]

[1] Viet Duc Industrial College, Song Cong City, Thai Nguyen Province, Viet Nam.
[2] Thai Nguyen University of Economics and Business Administration, Thai Nguyen Province, Viet Nam.Corresponding Author: Pham Hong Truong

ABSTRACT

The application of information technology has greatly changed people's work and life. At the same time, the importance of computer network security has become increasingly prominent. This article first analyzes the influencing factors of computer network security, and then conducts research on virtual network technology and its application in computer network security. The research shows that strengthening computer network security and protecting user information security are the focus of the current application process of computer network technology. content to focus on. Virtual network technology is an important way to improve computer network security, plays an important role in security assurance, and can better meet the actual security needs of users.

Keyword: Computer; Network security; Virtual network technology

1. INTRODUCTION

In the actual development process of computer network security work, virtual network technology, as a public network security technology, can effectively overcome the limitations of physical location and use a simulated network environment for users to perform data access or download operations. This application method can Better protect the security of information data and documents during uploading and downloading. The application of virtual network technology in computer network security can not only improve the operating efficiency of computers, but also greatly ensure the security of computer networks and has certain economic and social benefits.

2. FACTORS AFFECTING COMPUTER NETWORK SECURITY

There are many factors that affect computer network security, the most important of which are reflected in the following aspects:

2.1. Computer viruses

The invasion of computer viruses is the most important factor in the use of computers. During the use of the computer, if the wrong code or instructions are used, it is likely to cause vulnerabilities in the computer system and provide an opportunity for computer viruses to take advantage of. When a computer system is invaded by a virus, it will not only cause the leakage of file information and data information in the computer network, but may also cause the computer network system to be paralyzed, making the computer system unable to work normally.

2.2. Illegal intrusion by hackers

Illegal intrusion by hackers is mainly a human operation. Some people with a high level of computer technology can use the vulnerabilities of the computer system itself to conduct artificial intrusions to destroy the data or system in the computer. Under normal circumstances, hackers' illegal intrusion mainly includes two methods. One is to install viruses in computer software. When computer users download the corresponding computer software containing viruses, the computer system will be invaded by viruses, resulting in Computer systems are compromised to varying degrees, and the data and information in the computer systems will also be stolen. Another way is to use undefended paths in the computer network to invade the computer system and destroy the data files in the computer system.

2.3. Data eavesdropping and interception

Data eavesdropping and data interception in computer network security are also important means of leaking data information in computer systems. In computer networks, individual users

or enterprise users need to share resources and communicate through information transmission, but users cannot control the security of the information transmission process, so that the data is eavesdropped or intercepted during transmission. In particular, important user information such as personal identity information, bank card information, and corporate transaction information are more susceptible to interception and theft. At the same time, if the computer system itself ages or the computer hardware system equipment fails, it will provide opportunities for data eavesdropping and interception, leading to the occurrence of computer network security incidents.

3. VIRTUAL NETWORK TECHNOLOGY

Virtual network technology, as a public network security technology, has been widely used at this stage, and research on its concepts and specific applications is of positive significance.

3.1. Concept of virtual network technology

The difference between a virtual network link and a traditional network connection is that it does not use physical connections such as network cables, but uses a virtualized network to realize the connection between computer systems and realize the transmission and exchange of data information. Among them, there are two commonly used virtual network forms, one is a protocol-based virtual network, and the other is a virtual device-based virtual network. Virtual network technology can manage network transmission at specific locations according to different division standards, but data cannot be transmitted and communicated between different virtual networks. Therefore, virtual network technology has good security functions and can also protect data. transmission speed and transmission efficiency.

3.2. Application types of virtual network technology

3.2.1. Information security encryption technology

Information security encryption technology is a commonly used data encryption protection measure. The main principle is to encrypt and protect the data that needs to be transmitted. The encryption methods include encryption algorithms, data language operations, etc. The data information is not allowed to be transmitted to the computer until it is encrypted. In network systems, when data information is used again, corresponding data decryption is required to obtain the original data information. Information security encryption technology can not only ensure the security of data information, but also effectively improve the accuracy of data information. Therefore, information security encryption technology has a wide range of applications and has strong practicability.

3.2.2. Tunnel safety technology

Tunnel security technology is essentially a data encryption technology. Its basic working principle is completed through the cooperation of encryption protocols and network hardware devices such as routers to achieve secondary encryption of transmitted data, so that the transmitted data can be securely protected. Enter the computer public network system. Data transmission in a virtual private network can also be processed through tunnel security technology. The entire data information encryption and transmission process requires professional operation by professionals. The software and hardware equipment involved include virtual networks, tunnel terminators, switches, openers, etc. These links have been security optimized to ensure the safety and reliability of the virtual network environment.

3.2.3. Identity authentication technology

The application of identity authentication technology is to establish and manage the identity of relevant user information. Not only is a special account and password set in the virtual network system, but the user also needs to set up a corresponding user name and password independently. When a user needs to log in to the computer system, he or she must enter a username and password before proceeding with subsequent data operation instructions. At the same time, throughout the entire data transmission and conversion process, identity authentication technology can be used to verify the user's identity to ensure that relevant system operations and data transmission are implemented independently by the user, and the entire operation process is safe and controllable.

3.2.4. Key security technology

Commonly used key security technologies include public key and private key technology. In the actual application process of public keys, two keys need to be constructed. One key is used for data management of the public network, and the other key is set up and kept by the user independently. When data information needs to be transmitted in a public network, the public key must first be used to upload and download the data to ensure that the entire data transmission process is encrypted. After the user downloads it, the private key is used to decrypt it. Obtain the original data information. The private key is only used by the receiver and transmitter of the data to facilitate the encryption of data information. At the same time, the exchange of private keys is realized manually offline and does not go through the computer public network. Therefore, the use of private keys has minimal impact on computer network security.

4. SPECIFIC APPLICATIONS OF VIRTUAL NETWORK TECHNOLOGY IN COMPUTER NETWORK SECURITY

The specific application of virtual network technology in computer network security is mainly reflected in three aspects: the application of IPSecVPN technology, the application in computer network transmission, and the application in optimized firewalls.

4.1. Application of IPSecVPN technology

IPSecVPN technology is a key technology in virtual network technology. Its specific application refers to using VPN technology to achieve the establishment and connection of IP addresses after the computer system executes the IPSec protocol, thereby ensuring the security of data transmission by improving the accuracy of the computer IP address. This is mainly because the processing of data information in computer systems involves IP addresses. The IP addresses used by different enterprises, office areas and even departments are different, the transmission and communication of business data between each other requires the association of IP addresses between various networks to ensure smooth and safe data transmission channels. Therefore, the application of IPSecVPN technology is very necessary. In addition, when different enterprises and different users exchange data information through public networks, tunnel technology can also be used to encrypt data information to ensure the security of data information in the public network.

4.2. Application in computer network transmission

In actual operation, computers are often divided into multiple local area networks, and the transmission of data information between these networks can be achieved with the help of virtual networks. The application of virtual networks helps to establish correlations between various local area networks and form a complete network system according to the actual needs of users, so that users can realize the transmission and sharing of data information between various network systems. At the same time, virtual network technology can not only be used to connect local area networks, but also provide unified and centralized management of the network system. Through virtual network technology and user work needs, a computer system can be specifically and professionally set to increase the data transmission speed of the computer system. In addition, virtual network technology can also encrypt data information in the network system to ensure the security of network data. Virtual network technology helps build a relatively mature network architecture, which provides an important foundation for computer network security management and facilitates the establishment of scientific and orderly data transmission rules during the operation of computer systems. In practical applications, virtual network technology can also be used in conjunction with security measures such as network keys and firewalls to further enhance the security of data information during transmission.

4.3. Application in optimizing firewalls

Firewalls are an important channel for connecting software and hardware in computer systems. Therefore, firewalls are also a key system to ensure the security of computer network data. Firewalls can actively and effectively block conventional risk problems in computer systems. For example, when Trojans, viruses, hackers, etc. invade computer systems, firewalls can play a certain role in defense and blocking. The effective integration of virtual network technology and firewalls can optimize the firewall in the computer system to a certain extent. Especially when the

firewall in the computer system has loopholes and cannot effectively block the intrusion of viruses or hackers, virtual network technology can effectively make up for this shortcoming. Virtual network technology can ensure the security of data information by encrypting the information data in the computer network. At the same time, it can also assist the firewall to implement necessary encryption procedures to further consolidate the security barriers of computer network data. Generally speaking, the application of virtual network technology helps to optimize and strengthen the firewall system, and effectively avoids computer network security problems caused by too weak firewalls. The application of virtual network technology can optimize the performance settings of firewalls and also help improve the security performance of the entire computer network. Therefore, relevant technical personnel need to strengthen the joint application between virtual network technology and firewall systems to promote the optimization and update of firewalls.

5. APPLICATION OF VIRTUAL NETWORK TECHNOLOGY IN ACTUAL ENTERPRISES

When virtual network technology is applied in actual enterprises, it is mainly reflected in the application within the enterprise, the application between the enterprise and users, and the application between the enterprise and employees.

5.1. Application of virtual network technology within enterprises

There are business intersections between various subsidiaries or departments within an enterprise, which require the transmission and exchange of data services through computer network systems. However, most enterprises have many management structures and management departments, which makes the business The content is complex, which requires ensuring the security of the computer network. While ensuring efficient communication between different departments, it also pays attention to the confidentiality of corporate business information. Otherwise, once the company's important business information or commercial privacy is leaked, the company and even the entire industry will suffer a certain degree of economic losses. Therefore, the application of virtual network technology is to further enhance the security of enterprise network systems. On the one hand, the application of virtual network technology can effectively ensure efficient communication between different functional departments within the enterprise, strengthen the security and privacy of departmental connections, and build a healthy and safe corporate communication system. In this way, the parallel management and mutual coordination between various departments within the enterprise can be guaranteed, greatly reducing problems such as low work efficiency and high investment costs caused by inefficient interaction between different departments. On the other hand, the application of virtual network technology is also conducive to the management of enterprise managers. Enterprise managers can use virtual network technology to supervise and manage the work of subordinate employees in real time, strengthen the avoidance of work risk issues, and Ensure the smooth progress of all corporate tasks and strengthen the security of corporate internal management.

5.2. Application of virtual network technology between enterprises and users

The development of all business tasks of an enterprise requires necessary communication with customers. Therefore, the process of communicating with each other will involve the transmission and interaction of a large amount of data and information. The application of virtual network technology can effectively ensure the security of these data information. One of the more common security measures is to encrypt these files. The application of virtual network technology can achieve remote access through encryption technology or address translation technology, so that the security of enterprise user information can also be guaranteed. At this stage, important data within Vietnamese enterprises generally use encryption technology for security protection. Among them, virtual network technology is the most widely used in order to encrypt important data and information within the enterprise. Key information and data within the company or between the company and users will also be processed and transmitted using encryption technology to ensure that the company's important data and customer key information will not be maliciously stolen. In addition, in modern society, people's consumption will be realized through online transactions, such

as mobile banking, WeChat payment, Alipay payment, etc. The realization of these transaction payments needs to be carried out while ensuring the security of the network information environment. Therefore, using tunnel technology It is also necessary to use encryption technology to further ensure the security of online payment transaction operations. Most of the financial transactions between enterprises and users are conducted online, and the application of virtual network technology provides an important guarantee for the security of enterprise capital flows.

5.3. Application of virtual network technology between enterprises and employees

In the actual operation and management process, enterprises also need to pay close attention to the working status and work quality of their employees, and the application of virtual network technology provides important security measures for enterprise management. In the process of information exchange and communication between enterprises and employees, if important information or confidential information of the enterprise is involved, effective security protection will be provided with the support of virtual network technology to avoid the problem of employees leaking enterprise information. Therefore, the application of virtual network technology makes the communication between enterprises and employees more secure. At the same time, using virtual network technology to enhance the firewall performance of enterprise computer network systems can not only ensure the security of data transmission information between enterprises and employees, but also protect the system login information and related personal privacy information of enterprise employees, so that , when there is business data and information transmission between enterprises and employees or between employees and employees, virtual network technologies such as tunneling technology and encryption technology can effectively protect data information from being stolen, so that enterprise information is fully secure.

6. CONCLUSIONS

In summary, with the development of the information age, the computer network environment has become complex and ever-changing. Strengthening computer network security is an important measure to meet user needs and promote social development. The construction of a computer network security environment effectively ensures the security, sharing and efficiency of network data and information, and provides security guarantees for the development of individual users and society. At the same time, computer network system technicians also need to continue to develop and innovate more advanced and scientific virtual network technology to cope with the complex and ever-changing computer network environment and create a more secure virtual network system.

REFERENCES

[1] He Z, 2021, Application of Computer Network Security Technology in the Era of Big Data. Software, 42(10): 87–89.
[2] Hong Zhi Huang (2024). Research on the Application of Data Encryption Technology in Computer Network Communication Security. Applied Science and Innovative Research 8(2):p80. DOI:10.22158/asir.v8n2p80
[3] Kun Qi (2022). A Research on the Application of Virtual Network Technology in Computer Network Security. Journal of Electronic Research and Application 6(4):1-6. DOI:10.26689/jera.v6i4.4153
[4] Liu Z, 2021, Application of Firewall Technology in Computer Network Security. Electronic Technology and Software Engineering, 2021(23): 238–239.
[5] Yang L, 2021, Application of Data Encryption Technology in Computer Network Security. Wireless Interconnection Technology, 18(23): 20–21.
[6] Zhong Y, 2021, Application of Data Encryption Technology in Computer Network Security. Industry and Science Forum, 20(19): 35–36.
[7] Zhou Yun, Lu Rui (2020). Research on the Application of Virtual Network Technology in Computer Network Security. The 2020 International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy, SPIoT-2020, Volume 2 (pp.199-204). DOI:10.1007/978-3-030-62746-1_29