The Effect of Virtual Network Technology in Computer Network Security

Tianyu Bai

Wenzhou-Kean University, Wenzhou, Zhejiang, China

Abstract: In the daily operation of computer network, data security problems such as theft, network instability and connection failure often occur, which pose a serious threat to data security. With the continuous expansion of the application scope of computer technology, the problem of network security has become more and more complex. The emergence of virtual network technology provides a new idea to solve the problem of network security. Through virtualization technology, computer networks can be effectively isolated management between different local area networks, to realize the security of data transmission, so as to improve the security of the network. Virtual network technology can ensure the safe flow of information in the virtual network, and improve the operation efficiency of the network through the flexible network architecture design. Therefore, exploring the effect of virtual network technology in computer network security has become an important topic to be studied urgently.

Keywords: Computer Network Security; Virtual Network Technology; Function Effect

1. Introduction

In the tide of the digital age, the rapid development of virtual network technology has changed the way of information transmission, but also profoundly affected the pattern of network security. With the popularization of Internet applications, the traditional network architecture has been difficult to meet the increasingly complex security needs, virtual network technology emerged at the historic moment, become an important means to ensure information security and optimize the allocation of network resources. Virtual network technology, through the isolation mechanism, makes the physical network resources can be used effectively, and provides a more secure management mode.

2.The Main Types of Virtual Network Technology

2.1 Information Security and Encryption Technology

Information security encryption technology adopts advanced encryption algorithm to encode sensitive information, and only authorized users can obtain the raw data through decryption. Information security encryption technology plays an important role in the traditional data transmission security, especially in the cloud computing and software defined network (SDN) and other modern network architectures. In the cloud computing environment, information encryption technology can effectively protect the data stored in the cloud. Even if the data is maliciously accessed, it will always be encrypted to ensure information security. By using encryption means such as the TLS / SSL protocol, all data transfers between the client and the cloud server can be protected during transmission, avoiding the risk of data leakage. As an emerging network architecture, software-defined network (SDN) also relies on information security encryption technology to ensure the security of its network control layer and data forwarding layer. The SDN architecture provides more flexible network management by separating the control layer from the data layer, but it also brings potential security risks. Therefore, in SDN, information encryption technology is used to encrypt and control messages, prevent malicious tampering, and ensure the security of network configuration. Through the application of encryption technology, the information security in the virtual network environment has been significantly improved, and the data protection of the network architectureThe ability has also been further increased

2.2 Tunnel Safety Technology

Tunnel security technology is usually applied in the virtual private network (VPN) to provide a secure communication channel for users. In the tunnel security technology, the security of data transmission not only depends on the encryption algorithm, but also needs the synergy with routers, switches and other network equipment to further enhance the data protection through secondary encryption. Tunnel technology can effectively prevent malicious users from destroying the confidentiality of data by stealing data or tampering. During implementation, the tunnel terminal, opener, and other network management devices together build a secure transmission foundation, ensuring that data is not subject to unauthorized access or leakage during transmission. At the same time, the tunnel technology also has the integrity verification function of the integrity of the data package, which can detect whether the data is tampered with during the transmission process and ensure the authenticity of the data.

2.3 Identity Authentication Technology

In the traditional identity authentication, users authenticate by entering user names and passwords, but with the increasingly complex means of network attacks, a single user name and password has been unable to meet the increasingly severe security requirements. Therefore, the modern identity authentication technology has gradually developed a variety of more secure and complex authentication methods, including biometric identification technology, multi-factor authentication and digital certificate and other methods. In the application scenario of virtual network, identity authentication is not only to prevent unauthorized access, but also to ensure the security of sensitive data and operations. For example, in cloud computing and remote access environments, enhanced identity authentication measures can effectively prevent hackers or criminals from making malicious access by stealing user passwords or credentials, ensuring the integrity of data. In particular, multi-factor authentication technology significantly improves security by requiring users to provide additional authentication factors in addition to the user name and password, such as SMS verification code, fingerprint recognition or facial recognition. The additional authentication step increases the difficulty of illegal access and greatly reduces the security risks. And the identity authentication technology is also widely used in the whole process of data transmission and information processing, to ensure that every operation is confirmed by the legal identity, so as to avoid the data tampering and leakage in the transmission process.

2.4 Key Security Technology

Key security technology is an encryption system based on the public key and the private key. The public key is used to encrypt the data and can be publicly transmitted, without worrying about the data being interpreted by an unauthorized third party, because only the recipient with the corresponding private key can decrypt the data. The private key is kept separately by the receiver, as the decryption key, which can only be used to decrypt the data encrypted through the public key, ensuring that even if the data is intercepted in the transmission process, the unauthorized personnel cannot access the information. Specifically, when the sender needs to send the data to the receiver, the data should be encrypted through the public key of the receiver to ensure that even if the data is stolen during the transmission process, the attacker cannot decrypt the read. When the data reaches the destination, the receiver uses its own private key to decrypt the encrypted data and restore it to the original information. In order to ensure the security of the key, the private key exchange generally adopts a more secure way, not through the network transmission. Usually, the private key exchange is conducted offline, such as through physical media or face-to-face methods, to avoid the key being stolen during transmission. The application of key security technology is not only used in the traditional encrypted communication, but also widely used in e-commerce, cloud computing and financial transactions, and has become one of the important technologies to ensure information security and protect privacy.recent yearsWith the development of key security technology, according to the research statistics of Baijian Strategy (DIResaerch), the global cryptographic key management market size shows a trend of steady expansion. In 2024, the global cryptographic key management market size will reach 11.77 billion yuan, and is expected to reach 30.19 billion yuan in 2030, and the compound annual growth rate (CAGR) during 2024-2030 is 17.00%. North America and Asia Pacific are the main markets, accounting for about 74.8% of the global market share. As shown in **Table 1**.

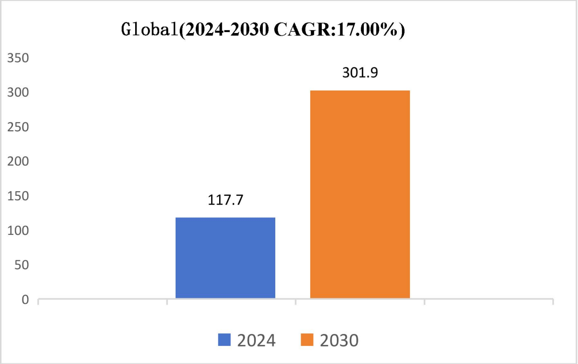

Table 1. Global Encryption Key Management Market Size (in RMB 100 million)

3. The Effect of Virtual Network Technology on Network Security

3.1 Improve the Scalability of the Network

Traditional network architectures are often limited by physical hardware resources, and expanding networks usually requires large-scale hardware investment. The virtual network makes the network resources can be flexibly expanded on demand through virtualization technology. When the network load increases, the virtual network can quickly meet the demand by dynamically allocating virtual resources, thus avoiding the bottleneck problem caused by the hardware capacity limitation in the physical network. In terms of network security, the virtual network can deal with various sudden security threats. For example, in the case of traffic attacks, the virtual network can quickly increase the bandwidth or adjust the traffic path as needed to ensure that important data is not affected. At the same time, the scalability of the virtual network is also reflected in its ability to automatically create isolated virtual local area networks (VLAN) and subnets according to the actual needs, which further strengthens the security protection ability of the network, avoids the spread of attacks to the whole network, and improves the self-healing ability of the network.

3.2 Reduce the Threat of Cyber Attacks

Through virtualization technology, virtual networks can separate different types of network traffic, data and applications, forming a multi-level protective barrier. Each virtual machine or virtual network instance can run separately in a virtual environment, limiting the possibility for an attacker to break through the entire network through an entry point. For example, virtual network can provide independent security policy for each virtual machine through virtual firewall, intrusion detection system (IDS), intrusion defense system (IPS), and make dynamic adjustments according to the changes in network traffic. The attacker breaks through the security protection of a virtual machine, and still cannot easily enter other virtual machines, because each virtual machine is strictly isolated. At the same time, virtual network technology can also provide automatic attack protection functions, such as automatic isolation policy generation, automatic network path switching, etc., to quickly respond to large-scale distributed denial of service (DDoS) attacks or other network threats.

3.3 Enhance Data Protection

Virtual network can ensure the security of data during transmission through virtual private network (VPN), encrypted tunnel and other technologies. The isolation nature of the virtual network allows the data to be isolated in a virtual environment, preventing unauthorized access. For example, sensitive data can be transmitted encrypted through a dedicated virtual network channel, avoiding exposure in the public network. At the same time, the virtual network can implement fine-grained access control policies, and only authorized users or devices can access specific data resources, thus greatly improving the protection of data. In addition, virtual network technology by storing data in a virtual environment, users can achieve fast data backup and recovery, in the event of security events, can quickly restore the normal operation state. The distributed storage nature of virtualization technology enables automatic backup synchronization of data between multiple physical nodes, increasing the availability of data recovery.

3.4 Improve Cost-Effectiveness

Virtual networks provide a significant improvement in security and are highly cost-effective. Traditional network construction needs a large number of physical equipment to support, and the construction and maintenance costs are high. The virtual network technology is integrated into a small number of physical devices through the virtualization of multiple virtual resource pools, which greatly reduces the input cost of hardware. Enterprises can dynamically adjust the allocation of virtual resources according to their actual needs to avoid the waste of resources. At the same time, the centralized management of the virtual network makes the network management become more efficient. Administrators can remotely manage the topology, configuration, and security policies of the entire virtual network through a unified control platform, thus saving a lot of labor costs. Through automated resource allocation, virtual networks can maximize the efficiency of the use of network resources and reduce unnecessary energy consumption. For example, virtualized servers and storage devices can increase utilization through resource pooling and reduce the need for physical hardware. With the continuous development of virtual network technology, its advantages in improving network security, reducing operation and maintenance costs, and improving resource utilization efficiency are expected to be further revealed.

4. Conclusion

With the rapid development of modern Internet, the threat of network security is becoming increasingly severe. From traditional data transmission encryption to modern cloud computing environment and software-defined network, technological progress has brought higher security requirements, promoting the continuous improvement of identity authentication, key management, tunnel encryption and other technologies. In todays highly developed information and digital era, network security involves every user, every system and every equipment. Virtual network technology improves the security of data transmission and reduces the risk, but also makes us realize how to balance the complex relationship between convenience and security, cost and effect. With the integration of emerging technologies such as artificial intelligence, network security will no longer be a single means of protection, but an intelligent and integrated defense system. For technology developers, how to find a balance between security and innovation to ensure that the system can prevent potential threats while maintaining efficiency, convenience and innovation will be a topic we will continue to explore.

References

[1] Lin Yi Building. Exploring the Application of Virtual Reality echnology in Computer Network Security Teaching in Higher Vocational Colleges [C] / / 2024 Lean Digital Innovation Conference Parallel Special Conference —— Collection of Metallurgical Industry Special Conference (Volume 2). 2024.

[2] Zhong Wei. A preliminary study on the role of Virtual network technology in Computer Network Security [J]. Mobile Information, 2023 (6): 198-200.

[3] Xian Zifu. Analyze the information security and protection under the computer network [J]. Information Industry Report, 2024 (4): 78-80.

[4] Jiang Zhongjun, General Zhao. Analysis of computer network information security technology and development trend [J]. Communication World, 2024 (5): 73-75.