ISSN: 2424-8460(O)
2251-2608(P)

Original Research Article

Research on the application of virtual network technology in network information security protection

Hong Qiu
Chinese People's Police University, Langfang, Hebei, 065000, China

Abstract: With the rapid development of digital technology, network information security has become a core issue affecting social operation and enterprise development. Traditional network security protection methods have shortcomings such as poor flexibility and high deployment costs, making it difficult for them to adapt to the dynamic and complex modern network environment. As a new type of network architecture technology, Virtual Network Technology (VNT) possesses characteristics including resource virtualization, flexible deployment, and isolated operation, providing a new solution for network information security protection. This paper expounds on the core technologies of VNT and focuses on exploring its application scenarios in security protection, such as remote access security, network isolation, and attack defense. Research shows that VNT can effectively improve the flexibility, scalability, and security of network systems, and has broad application prospects in the field of network information security.
Keywords: virtual network technology; network information; security protection

1. Introduction

In the context of the global digital transformation, networks have become an important infrastructure for governments, enterprises, and individuals. However, while networks bring convenience, they also face increasingly severe security threats, such as data leakage, ransomware attacks, and DDoS (Distributed Denial of Service) attacks. Virtual Network Technology (VNT) breaks the limitations of traditional network architecture by abstracting physical network resources (such as servers, switches, and routers) into virtual resources. It allows multiple virtual networks to run independently on a single physical network, and each virtual network can have its own security policies and access controls. This characteristic makes VNT show unique advantages in network information security protection. Therefore, studying the application of VNT in network information security protection is of great significance for improving the overall security level of the network [1].

2. Core technologies of virtual network technology

2.1. Virtual private network (VPN)

VPN is a technology that establishes a secure encrypted communication channel between remote users or branches and the enterprise intranet through a public network (such as the Internet). Its core principle is to use encryption protocols (such as IPSec, SSL/TLS) to encrypt data transmitted over the public network, preventing data from being intercepted or tampered with. VPN can be divided into three types according to the application scenario: Access VPN (for remote individual users), Site-to-Site VPN (for inter-branch communication), and Extranet VPN (for communication between enterprises and partners). In terms of security, VPN not only ensures

ISSN: 2424-8460(O)
2251-2608(P)

data confidentiality but also verifies the identity of users through authentication mechanisms (such as username/password, digital certificates), effectively preventing unauthorized access [2].

2.2. Software-defined networking (SDN)

SDN is a network architecture that separates the control plane and data plane of the network. In the traditional network, the control function and data forwarding function of network devices (such as routers) are integrated. In the SDN architecture, the control plane is concentrated on a centralized controller, and the data plane is composed of simple forwarding devices. The controller can dynamically adjust the forwarding strategy of the data plane according to the network status and security requirements. This separation makes the network more flexible and manageable. In terms of security protection, the SDN controller can monitor the entire network traffic in real time. When abnormal traffic (such as DDoS attack traffic) is detected, it can immediately issue instructions to the forwarding devices to block the attack source, achieving rapid response to security threats [3].

2.3. Network functions virtualization (NFV)

NFV refers to the technology that virtualizes traditional hardware-based network functions (such as firewalls, load balancers, and intrusion prevention systems) into software applications running on general-purpose servers. Compared with traditional hardware devices, virtualized network functions (VNFs) have the advantages of fast deployment, flexible scaling, and low cost. For example, when the network traffic increases sharply, enterprises can quickly deploy multiple VNF instances through virtualization technology to enhance the processing capacity of security functions; when the traffic decreases, they can shut down redundant instances to save resources. In addition, NFV supports the dynamic combination of VNFs. Enterprises can customize security service chains (such as "firewall + intrusion detection + data encryption") according to their own needs, improving the pertinence of security protection.

3. Application scenarios of virtual network technology in network Information security protection

3.1. Remote access security protection

With the popularity of remote work models (such as telecommuting and mobile office), the security of remote access to the enterprise intranet has become a key concern. Traditional remote access methods (such as dial-up access) have low transmission speeds and poor security, making them vulnerable to man-in-the-middle attacks. VPN technology can solve this problem well. Remote users only need to install VPN client software on their devices (such as laptops, mobile phones) and connect to the enterprise VPN server through the Internet. After identity authentication, an encrypted communication channel is established. In this channel, all data (such as work documents, customer information) transmitted between the user and the intranet is encrypted, ensuring that even if the data is intercepted by attackers, it cannot be decrypted and used. For example, during the COVID-19 pandemic, more than 80% of Fortune 500 companies used VPN to provide secure remote access services for employees, and the incidence of data leakage caused by remote access decreased by 62% compared with before [4].

3.2. Network isolation and security domain division

In complex network environments (such as enterprise intranets, government networks), different departments

ISSN: 2424-8460(O)
2251-2608(P)

or business systems have different security requirements. For example, the financial department's network needs higher security than the marketing department's network, and the core business system needs to be isolated from the general office system to prevent cross-domain attacks. VNT can realize flexible network isolation through virtual network segmentation. Taking SDN technology as an example, the controller can divide the physical network into multiple independent virtual networks (called "virtual slices") according to the department or business type. Each virtual slice has independent network resources and security policies, and there is no direct data interaction between slices. Even if one virtual slice is attacked, it will not affect other slices. In addition, NFV can deploy dedicated security VNFs (such as intrusion prevention systems) for each virtual slice to further enhance the security of the slice.

3.3. Active defense against network attacks

Traditional network attack defense is mostly passive (such as relying on firewalls to block known attack signatures), and it is difficult to deal with unknown attacks (such as zero-day vulnerabilities). VNT, especially the combination of SDN and NFV, can realize active defense against attacks. On the one hand, the SDN controller can collect real-time traffic data from the entire network, analyze the traffic characteristics through machine learning algorithms, and identify abnormal behaviors (such as sudden increases in traffic, abnormal access paths) that may indicate attacks. On the other hand, once an attack is detected, the controller can quickly call the corresponding VNFs (such as DDoS mitigation devices, virus scanning software) through the NFV platform to form a dynamic defense chain. For example, when a DDoS attack is detected, the SDN controller can first redirect the attack traffic to a virtual cleaning center (composed of multiple DDoS mitigation VNFs) to filter out malicious traffic, and then forward the normal traffic to the target server. This active defense method can reduce the impact of attacks on the network.

3.4. Secure backup and recovery of data

Data is an important asset of enterprises, and data loss or damage caused by natural disasters, hardware failures, or malicious attacks will bring huge losses to enterprises. VNT can provide a secure data backup and recovery solution through virtualization technology. On the one hand, enterprises can use NFV to deploy virtual backup servers. These servers can automatically back up important data at regular intervals, and the backup data is stored in an encrypted manner to prevent unauthorized access. On the other hand, when data loss occurs, the virtual backup server can quickly restore the data to the target device through the virtual network. Compared with traditional physical backup devices, virtual backup servers have the advantages of fast backup speed and low cost. For example, a multinational enterprise used NFV-based data backup technology to reduce the data backup time from 8 hours (traditional physical backup) to 1.5 hours, and the cost of backup equipment was reduced by 40%. At the same time, due to the encrypted storage of backup data, there was no data leakage incident during the backup process.

4. Conclusion

This paper studies the application of Virtual Network Technology (VNT) in network information security protection. It is found that VNT (including VPN, SDN, and NFV) can effectively solve the problems of traditional network security protection, such as poor flexibility, high cost, and passive defense. In remote access

ISSN: 2424-8460(O)
2251-2608(P)

security, network isolation, attack defense, and data backup, VNT shows obvious advantages, which can improve the security, flexibility, and efficiency of the network system.In the future, with the continuous development of virtualization technology, artificial intelligence, and 5G, VNT will become more mature. It is expected that VNT will not only be applied in enterprises and government agencies but also play an important role in emerging fields such as smart cities and industrial Internet, providing a more solid security guarantee for the development of the digital economy.

References

[1] Zheng Y ,Wang L . Application of entertainment virtual technology based on network information resources in piano teaching [J]. Entertainment Computing, 2024, 50 100675-.

[2] Dany P K B ,Binele A A ,Emmanuel T , et al. Optimizing Telematics Network Performance through Resource Virtualization in a Disruptive Environment: The Case of the IP/MPLS Core Network [J]. Network and Communication Technologies, 2023, 8 (2): 1-.

[3] Zhe Z ,Xintong J . A Virtual Net Locks Me In: How and When Information and Communication Technology Use Intensity Leads to Knowledge Hiding. [J]. Journal of business ethics : JBE, 2022, 187 (3): 11-16.

[4] ZhongBao W ,WenMing L ,GuoQing W . Information Steganography Technology of Optical Communication Sensor Network Based on Virtual Reality Technology [J]. Journal of Sensors, 2022, 2022.