# Research on the firewall of smes based on Ipv6 technology

*Chuanzhong Xie[1], Bo Feng[2], Guofeng Zhang[1], Chao Wang[2]*
1. Jiangxi Branch of China Telecom Corporation Limited, Nanchang 330029, China
2. Jiangxi Branch of National Internet Security Administration Center, Nanchang 330038, China

**Abstract:** The rapid development of network technology provides an opportunity and convenience for all walks of life, but also promotes the enterprises to begin to information operation and management construction. It is precisely because the Internet environment is becoming more and more complex, so the problem of network threats has gradually attracted people's attention, especially some small and medium-sized enterprises network security problems are more prominent. Ipv6 is developed on the basis of Ipv4, which provides enterprises with more network addresses to choose from, which can solve the problem of insufficient network address resources from the root. With the help of Ipv6 technology, this paper analyzes the design of small and medium-sized enterprise firewall, in order to highlight the technical advantages of Ipv6. This paper first analyzes the related concepts, then briefly expounds the firewall architecture and function allocation, and finally puts forward the firewall construction scheme to improve the network anti-risk ability.

**Key words:** Ipv6 technology; Small and medium-sized enterprises; Firewalls

## 1. Related concepts

1.IPv6 security protocol

InternetProtocolVersion6, also known as IPv6, is an Internet IP protocol based on the Network Engineering Task Force (IETF). The IPv6 security protocol defines the three main types of Internet addresses: unicast, multicast, and anycast. Unlike the previous generation IPv4 protocol, the broadcast address has been replaced by the anycast address. In IPv6, the broadcast function of the original IPv4 protocol is implemented in multicast mode. In particular, in the IPv6 security protocol, unicast addresses are used to identify a single interface through which data information will be identified. A multicast address is a method of identifying interfaces in a network by which data is transmitted to the various interfaces identified by the multicast address. An anycast address can also be used to identify a group interface. The difference with a multicast interface is that data passing through an anycast interface will flow into a rearranged network address interface to which the nearest node is directed.

2. Technical advantages of IPv6 security protocol

Compared with IPv4, IPv6 has huge application advantages. Specifically, it is mainly reflected in richer geological resources, smaller routing table, enhanced multicast support, optimized flow control, and higher security performance. At the same time, the header format is more optimized, and the expansion performance also has a good advantage. It is reflected in the following points: First, compared with IPv4, IPv6 has 128-bit IP addresses, so the upper limit of IP addresses has been increased from 232 to 2128; Second, on the basis of IPv6, according to the clustering principle, on the basis of IPv6, the router only needs to call a single record from the route, it can identify a subnet. Therefore, the length of the routing table can be obviously reduced, and the efficiency of the router's data information processing can be improved to the greatest extent; Thirdly, under IPv6, the effective optimization of multicast and flow control can be realized to promote the development of new media and improve the quality of QoS of the network. Fourth, under the IPv6 protocol, the network has higher security performance, under the IPv6 protocol, users can carry out high-level encryption of data information and IP packet check, and under the password check option, the security and integrity of the packet have been optimized to the greatest extent; Fifth, compared with IPv4, the scalability of IPv6 has been optimized to a certain extent, so it becomes more convenient to expand and integrate new technologies and new functions.

3. Firewall

Firewall is a combination of various network security management methods, and the use of a number of network protection software and hardware of a network protection system, it can build a layer of security barriers between the local area network and the Internet, according to user requirements, set a variety of security levels, so as to ensure the security of user data and information, While the central enterprise can in the process of building the network firewall, the security risks existing in the Internet are timely detected. The security risks in the process of data transmission are effectively solved, and its security protection means include data isolation and data protection. In addition, it can also monitor and record various operational behaviors of users in the process of using the Internet. If unsafe network behaviors or abnormal attacks are found, security warnings will be given to users, and security measures such as local isolation will be made. Therefore, under the premise of ensuring the security and integrity of network users' data and information, firewall technology can effectively improve the experience of network users.

## 2. The IPv6 protocol under the small and medium-sized enterprise firewall technology theory

1. Overview of IPv6 Internet protocol

IPv6 is a new generation of Internet protocol updated from IPv4. On November 26, 2019, all IP addresses in IPv4 have been fully distributed, so future ISPs and some large network infrastructures must distribute IP addresses in accordance with IPv6. However, at present, IPv4 and IPv6 still coexist, and IPv4 and IPv6 will go through a long transition period together. The biggest advantage of IPv6 protocol is

that it has an extended order of magnitude of address space, using the 32-bit length of IPv4 protocol, the number of network addresses can be allocated to reach 4.3 billion, and using the 128-bit length of IPv6 protocol, the number of network addresses can be provided as high as 2128, under normal circumstances, this number is close to infinite. That is to say, in the IPv6 protocol, the number of network addresses that can be used is not limited. In addition, IPv4 appears IP connection problems, low network security, multicast problems have been well solved, mobility and quality of service has been significantly improved.

2.2 Security mechanism of IPv6 protocol

Due to the shortage of network address resources, IPv6 integrates IPSecurity, so in the foreseeable future, IPv6 will eventually replace IPv4 completely. The high security of IPv6 largely comes from the security mechanism of IPSec, which is centered on password and authentication, and password is to encode data information according to a certain law. In this way, even if the data is stolen, there is no risk of data leakage. Authentication means that the data receiver can verify the identity of the data sender and whether there are any unauthenticated changes to the data as it travels over the network.

2.3IPv6 Address Assignment Protocol

In IPv6, there are three types of addresses, namely unicast address, multicast address and anycast address. In IPv6 network, the IP address allocation in IP network needs to consider the routing performance, routing policy and security, and in the specific application, the IP address allocation in IP network adopts three ways: monotonous, sparse and random. It is most suitable for the address assignment technology such as assignment and prefix delegation. In IPv6, it also provides two types of automatic address setting protocols: one is the stateless automatic address setting protocol, and the other is the Dynamic Hosting protocol of IPv6. Among them, when the stateless address is used to automatically configure the protocol to assign the address, there is no need to intervene in the management of the server, you can use the router announcement information and the local MAC address to automatically assign, so as to obtain the IPv6 address of the machine. In the use of IPv6 dynamic host configuration protocol to configure the address, it is necessary to have a dedicated server to manage the address pool, only when the host issued a request to obtain an IPv6 address, it will automatically set the address.

## 3. The firewall based on IPv6 technology

1. Protective wall architecture

In IPv6, the firewall is composed of two parts: the client side and the client side. Among them, the firewall of the client side mainly screens and filters the data of the client side according to certain security criteria, so as to prevent virus intrusion and virus intrusion. The role of the security policy management server in network security is that it actively manages the events of network security, user behavior, network running log and system audit, etc. It can realize unified network management through centralized management and control, so as to improve network security. In addition, according to the backup mode of two physical layers of IPv6, the security of the system can be better improved.

2. Set the mode of the firewall

The design of the firewall system uses a bridge method, which can realize the bridge between the various networks of the firewall. Assume that SERVER1 firewall and SERVER3 firewall as the main firewall, SERVER2 firewall and SERVER4 firewall as the backup firewall. According to the firewall detection logic, then the primary firewall will be responsible for all the important network servers, and you can switch between the primary firewall and the backup firewall by modifying the firewall parameters.

3. Security policy of the firewall

In the modern firewall, its security policy is determined by the matching conditions, actions and security profile and other elements, its application scope is mainly for the network data flow process and data content for security integration monitoring. If the firewall monitors the behavior of computer access to the network and the set security policy is consistent, then the access behavior can be successfully realized, so that the data information can pass through the firewall. When the firewall determines that a threatening user enters the Internet, it will prevent them from entering the Internet. The criteria for matching an IPv6 firewall are source address, destination address, and source port. The destination port and protocol constitute the VLAN, source security zone, target security zone, user, time period, and so on.

## 4. IPv6 security upgrade measures

1. Strengthen policy support and strengthen security management

The “action plan” clearly puts forward specific requirements for IPv6 work in China, and puts forward corresponding policies and technical standards, and emphasizes the security issues in China’s IPv6 work. At the same time, it is necessary to strengthen the education and training of IPv6 related knowledge, improve the quality of practitioners, and pay attention to the security management of IPv6. Early research, early discovery and early solution should be done to nip the problem in the bud.

2. Increase investment in IPv6 research and deployment

First, due to the characteristics of the IPv6 protocol itself, it is vulnerable to fragment provisioning, neighbor discovery protocol attacks, extended header attacks, etc. It is necessary to conduct research on attack mechanism analysis, attack detection, attack defense, attack cracking and other aspects according to the characteristics of different attack types. Second, in the transition from IPv4 to IPv6, the transition mechanism and security considerations are combined, a smooth, seamless and secure transition technology is proposed, and a new design method of security system is proposed; Third, regarding the integration of new technologies and new applications, cybersecurity technologies in areas such as mobile Internet, Internet of Things and cloud computing should be studied in IPv6; Among them, for the

mobile Internet environment, the research focuses on the mobile security management of IPv6. For the Internet of Things environment, the research focuses on the perception layer security of IPv6; For cloud computing environment, focus on IPv6 security.

3. Accelerate the development of information security products

The relevant personnel of the enterprise can optimize and upgrade the network security guarantee system on the existing basis, and put forward corresponding solutions. According to the Action Plan, all kinds of security products should improve the ability to accurately locate, detect and strike IPv6 addresses and quickly process IPv6 addresses, and carry out ipv6-oriented network security level protection, personal information protection and risk assessment, disaster backup and recovery.

## Concluding Remarks

IPv6 is a new generation of Internet security protocol, which promotes the secure operation and development of the Internet. At the same time, for small and medium-sized enterprises, reliability, construction and operation costs, technical threshold, etc., are the main factors that affect the construction of enterprise-level firewalls. In the future, we should continuously optimize and reconstruct the structure of the network system, develop and use new network encryption technology, and comprehensively improve the security and performance at the network transport layer and application layer. Promote the development of enterprise network to a safer and more efficient direction, and ensure the normal operation of enterprise data services.

## References:

[1] Yaojun Ma. Effective Application of Firewall Technology in Computer Network Security [J]. Science and Technology Information,202,20(13):16-18.

[2] Lijing Gao. Application of Firewall Technology in Computer Network Security [J]. Network Security Technology and Application,2022(06):11-12.

[3] Hongying Li,Xiaoman Zhang,Tianrong Zhang. Network Firewall state Detection Model based on trust mechanism [J]. Computer Simulation,2022,39(04):428-432.

[4] Zhen Li. Security Design and Systematic Management of Computer Network [J]. Information and Computer (Theoretical Edition),2021,33(02):186-188. (in Chinese)