A dynamic port isolation method

Sun Tao¹, Wang Hai, Gao Yang
ZhangJiaKou Electric Power CO., LTD. 075000, China
zmr1990@sjtu.edu.cn

Abstract. With the rapid development of enterprise information construction, the enterprise internal network information interaction is frequent, which greatly improves the efficiency of enterprise work, but the problem of network security is increasingly serious. In view of the above problems, this paper proposes a port dynamic isolation method, which can complement the existing security tools, and provides an idea for solving the security of intranet.

1. Introduction
The rapid development of Internet technology has brought convenience to us, but at the same time, there are also threats to network security. According to the 45th statistical report on China's Internet Development released by China's Internet Information Center in 2020, by April 2020, the national Internet Emergency Center has detected and coordinated the disposal of 185573 tampered websites in China, including 515 government websites. A large number of researchers have carried out a lot of research in the field of network security, and established a defense system including firewall, intrusion detection and access control to ensure and improve network security. The continuous disclosure of network security incidents and their serious consequences still expose the problems of traditional network security defense, and the defense situation of "easy attack but difficult to defend" has been enlarged with the highlight of cyberspace security status. For example, information privacy leakage, especially the enterprise internal network, the data transmitted in the network is related to the vital interests of enterprises. So it is urgent to ensure the security of enterprise network from attack.

As an information infrastructure, enterprise internal network is an important platform for internal office. The structure of enterprise internal network is more complex, which leads to more security risks. From the perspective of LAN, there are four representative security threats

1. ARP attack. In LAN, the attacker uses the inherent loophole of ARP protocol to send the tampered ARP broadcast message by deception and disguise it as the MAC address of the target host, so as to hijack traffic or DDoS attack.

2. The broadband remote access server of enterprise network is gradually deployed to the network core, and the user access gradually evolves from static IP address allocation. Ipoe is realized by the way of DHCP address allocation. In the process of establishing connection, the gateway spoofing and traffic hijacking caused by private DHCP in the same broadcast domain cannot be avoided.

3. The broadcast storm caused by the loop at the access end. Due to the active users in the enterprise network, it is difficult to fully control the network behavior. The situation of the loop caused by the wrong connection of the LAN equipment often occurs. The broadcast storm caused by the loop will cause all terminals in the same broadcast domain to be unable to use the network normally, and even affect the forwarding performance of the three-layer equipment where the gateway is located, and then affect the entire network.
(4) The penetration of Trojan virus in LAN. The security measures of intrusion prevention system will be deployed at the network boundary, but it cannot prevent the computer virus from penetrating into the LAN. Especially in the absence of isolation in the LAN, the virus infected by a single terminal device tends to explode. If the server and the client are in the same LAN, if the server and the client are attacked, the loss will be huge. For example, the standard network service port provided by the server is always open in the whole life cycle to facilitate the client to access the service through the port. The static service model also exposes applications to potential attackers for a long time. Attackers can perform port network scanning, locate the system, obtain detailed information and start worms to destroy the network.

In view of the above problems, this paper proposes a dynamic port isolation method. For the logical port, the port used by the dangerous service is isolated to ensure that the virus will not infect other terminals through the network.

2. Related work
Ports in the network are generally divided into two categories[2]. One is the physical port, such as the interface used to connect the network cable on the switch, optical cat and router; the other is the logical port in the communication protocol, whose range is 0-65535, and the common ports are 80 and 21.

Port isolation technology is mainly through the configuration of the actual physical ports on the switch[3], so as to achieve sufficient isolation between the client ports, so as to ensure that one client will not receive traffic from another client. By using this technology, the controlled ports are added to the isolation group, so as to realize the data isolation between layers 2 and 3. It provides a solution for the flexible networking. After the port isolation, it can effectively avoid the spread of virus caused by unicast, broadcast and multicast, and can effectively prevent ARP attacks. In addition, Huawei, D-Link, Cisco and other manufacturers also provide configuration methods, and the port separation is easy to implement. If the configuration is cumbersome, it needs professionals to configure, and after isolation, the shared printing function cannot be realized, and can only be implemented on one switch, thus limiting the scale of the network

The existing port isolation technology mainly focuses on the physical port configuration of the switch, which is realized by dividing the isolation group[4], which is lack of flexibility. Aiming at the problem of insufficient flexibility, dynamic isolation of logical ports in communication protocol can not only improve communication flexibility, but also achieve port isolation and ensure terminal security[5,6].

3. A method of dynamic port isolation

![Diagram of port dynamic isolation method](image)

(1) Port table
The port table is divided into three parts according to the properties of ports: recognized ports (range 0-1023), registered ports (1024-49151) and dynamic private ports (49152-65535). Recognized ports are closely bound to specific service protocols and cannot be redefined. Most registered ports have no clear definition and need to be redefined according to different services. Trojan horse programs often have a port definition of this range. In theory, there will be no service to allocate the range port for dynamic private port.

(2) Port matrix

The registered port and the dynamic private port range constitute a one-dimensional matrix M. the range of matrix M is 0-65535, and its attribute value is 0 or 1, 0 means that the port is isolated, and 1 means that the port can be used. The initialization of matrix M is all 1.

A dynamic port isolation method is shown in Figure 1. Firstly, the IP address and port number are obtained by analyzing the protocols applied by both sides of the communication, and then the port numbers are counted according to the analysis results in the set time window, and the port numbers are sorted from high to low according to the number of ports. If the port value appears in the range of 0-1023, the port matrix will not be operated; if the port appears in the range of 1024-49151, the port position value corresponding to matrix M will be changed from 1 to 0, and the top 25% of the port occurrence times in this time window will be monitored; if the port appears in the range of 49152-65535, the port matrix will not be operated, perform the same operation as above, change the port position value corresponding to matrix m from 1 to 0, and monitor the port.

Port 0-1023 is closely bound with specific service protocols, and the existing security tools can effectively prevent the threat of this kind of port. Therefore, the method proposed in this paper does not operate the port in this range. Therefore, the first 25% ports in the time window are monitored and isolated. If there is a threat in the process of monitoring the port, the port will continue to be isolated until the threat is eliminated. If there is no threat, the corresponding port of matrix M is set to 1 and the port is released. The port is in the range of 49152-65535. It can be seen from the above that the ports in this range are rarely used. The possibility of Trojan horse is very high, so it is necessary to monitor and isolate the port. If it is found that there is a threat in the port during the monitoring process, the port will continue to be isolated until the threat is eliminated. If there is no threat, set the corresponding port of matrix m to 1 and release the port.

4. Summary

This paper summarizes and analyzes the technical methods of port isolation, and proposes a dynamic isolation method for logical port by analyzing the existing isolation technology mainly aiming at the operation limitation of physical port. Through the dynamic isolation of logical port, it can not only complement the existing security tools, but also improve the ability to face the threat of intranet security, and is not limited by hardware. It improves the network flexibility and enriches the connotation of port isolation technology theoretically.

References
[1] China Internet Network Information Center. The 45th statistical report on China's Internet development [R], 2020.
[2] Tang Lei, Tang Lei. Application of port isolation technology in campus network management [J]. Information security and technology, 2015 (7).
[3] Chen Song. Static IP address conflict prevention strategy based on port isolation [J]. Computer engineering and design (1): 75-77 + 85.
[4] Lin Chujian, Zhang Sihai, Wang Haiying, et al. Research and application of port isolation technology based on asymmetric VLAN [C]] the 12th Annual Academic Meeting of education informatization branch of China Association of higher education. 2014.
[5] Zhou Yuyang, Cheng Guang, Guo Chunsheng, et al. Research review of dynamic transfer technology of attack surface of mobile target defense [J]. Acta software, 2018 (9): 2799-2820.
[6] Luo Y B, Wang B S, Wang X F, et al. RPAH: Random Port and Address Hopping for Thwarting
Internal and External Adversaries[C]// 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015.