Design Idea of Small and Medium-sized Enterprise Network Based on Identity Authentication

Enning Yuan*

Shandong University of Science and Technology, Network Engineering, Intelligent Equipment College, Shandong, China

*Corresponding author: 551137070@qq.com

Abstract. With the rise of the digital era, more and more SMEs are springing up all over the country, and a network system adapted to SMEs has become an important factor affecting the development of their businesses. Therefore, more and more SMEs across China have accelerated the pace of building their own powerful and effective information network systems. Nowadays, face recognition technology has been gradually improved, and the application of face recognition technology has brought two sides to the network structure of enterprises. This paper designs the authentication mechanism of face recognition for different levels of IP, based on the IP restrictions between different levels, to achieve the isolation between companies and different levels, and to achieve the purpose of strengthening the security of network systems of SMEs.

Keywords: local area network; face recognition; IP authentication; security

1 Introduction

The IT industry is developing rapidly and has been widely used in many fields, among which, the reasonable planning of network planning and deployment for small and medium-sized enterprises has become an important development direction for enterprises, and the importance of the network system bearing their business data is gradually increasing. Nowadays, more and more small and medium-sized enterprises have attached importance to the construction of information technology platform and deeply recognized the necessity and urgency of enterprise network construction. With the development of information technology construction, more and more small and medium-sized enterprises have more and more widely adopted network information technology to expand their security functions. At present, there are still many difficulties in the process of SME network construction. As some SMEs do not consider their own requirements, or simply pursue high performance, the systems built are often unnecessary losses, on the other hand, some SMEs built systems themselves are not exactly the network of user needs, in terms of network security [1], SMEs also do not have completely reasonable countermeasures, these reasons may more or less add obstacles to the

V. Escudero et al. (Eds.): BADS 2022, AHCS 11, pp. 391–398, 2023.
https://doi.org/10.2991/978-94-6463-102-9_42

development of enterprises [2]. Therefore, while designing the network structure, these problems should be taken into account as a whole, and the face recognition technology, which is now popular and becoming mature, should be applied to the network construction, and the actual needs of enterprises need to be fully considered at the beginning of the network design, by the need to specifically design the network to meet the needs of their own enterprises [3]. At the same time, when setting up the LAN, the advanced nature of the Internet, security, and high-speed network bandwidth should be taken into account.

2 Requirement analysis

The enterprise consists of three divisions: Administration Department, technology Department, Sales Department and a number of other departments [8].The central machine room is located in the administration building. For ease of working, the Technical Department is located in the same building as the Sales Department [4], while the remaining department occupies one building. The private server of the company is connected by VPN, which provides the Email function for the Intranet and the storage of financial data and confidential company documents [5].The local resource server of the administration department provides the public information and shallow security files of the company. Some administrative department, technical department staff work location is not fixed, because of the internal reasons of the company, part of the administrative department and technical department staff work location in other departments [6]. To ensure security, all servers provided outside the company must be protected by firewalls. In order to better extend the network, it is required to leave some unallocated network segments for the enterprise [7].

3 Design a master plan

3.1 Master Plan

The design and implementation of the network system of the enterprise follow all the practical considerations, the principle of reasonable economic benefits, the overall plan is as follows:

The company's local area network takes into account the multi-layer core, and establishes a three-layer core router and a two-layer central switch to ensure the smooth transmission of data flow in peak hours. At the same time, the core devices need to maintain the necessary power backup and machine backup, in order to adapt to the network problems can maintain a safe and stable network work.

The company and the enterprise's subsidiary (or external enterprise) through the VPN connection, from the perspective of security and practicability, enterprise VPN port selection should avoid the common port number, the value of the port number can be determined according to the actual.

In view of the existence of other departments in the management personnel belonging to the administrative department or technical department, staff attendance records

and network security issues, consider the enterprise internal IP address is divided into temporary IP address and formal IP address, the purpose of temporary IP is: 1. The purpose of the temporary IP address is: 1. The interaction between the personnel of other departments 2. The temporary IP address serves as the carrier of the network layer of the data flow when the owner performs authentication (interaction with the facial database). The purpose of a formal IP is to distinguish it from a temporary IP. Formal IP interactions are logically isolated from the enterprise external network (temporary IP).

3.2 Post-Network Work

Both temporary IP and formal IP use variable length mask to make full use of IP address resources and achieve IP address clustering. IP addresses are divided into temporary IP addresses and official IP addresses based on requirements. The temporary IP address segment is expected to be A.X.0.0/16, where X is the number of each department, and the number of its subdepartments is A.X.Y.0/24. The numbering rules for subdepartments are the same as those for the temporary IP address segment. (The values of A and B can be determined separately according to actual requirements)

For all switches, scripts can be used to dynamically design all ports. For example, before authentication, the switch port to which the user is connected is Vlan 10, which can be adjusted based on the value returned by the face database: if ACK is returned, it will continue to be Vlan 10, and if a digital token is returned, Vlan will be set to 20.

Set all DHCP servers on the core switch and set the script: When a packet containing a digital token is received and its source address is a temporary IP, its destination IP is itself, it is judged to be correct. If yes, the DHCP server replies to the packet whose temporary IP address has expired and sends a packet containing a formal IP address.

For data packet interaction between departments, use the OSPF routing protocol on the active line and enable static routing on the standby line. The OSPF routing protocol is used because it supports two routes on the main line, so that load balancing and mutual backup can be achieved on two bidirectional routes. Of course, the link cost value of each link can be modified according to the specific situation to control the transmission path of data flows [9].

4 Design concept of network structure

In terms of overall structure, the enterprise network is divided into three parts: the external network, the internal network (referred to as the internal network for short) and the internal network. The external network uses temporary IP to communicate, while the internal network uses formal IP to communicate, and the formal IP can connect to the internal network through VPN [10]. The internal network stores the core technical data, financial data, etc. Considering that employees of other departments may need to access the Intranet [11], when adding temporary IP to access the Intranet, apply for the administrator authentication module first. Only after the administrator agrees and gives

the employee a time-limited VPN account, can the employee access the Intranet, as shown in Figure 1.

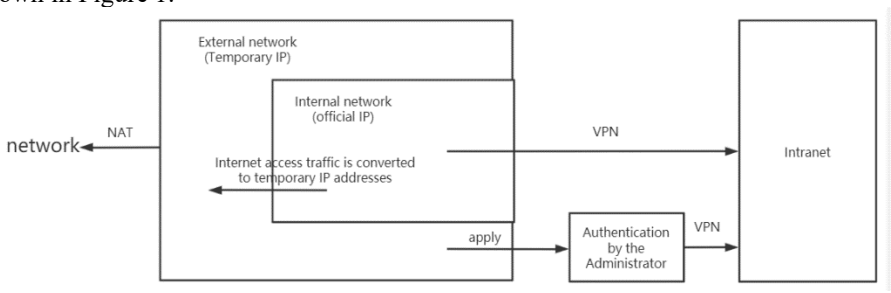

Fig. 1. Network structure design

5 Running module design

5.1 Employees get IP address module

After the client is opened, each module of the network system near the client will be activated, and the data stream will be read and operated through the call between each module. When obtaining the IP address, the client will be differentiated according to whether it is the first use of the client (Note: the first use here refers to whether it is the first use of the day, and the design client will update the login information of the last login to the local log file and refresh it 5 hours after being shut down) : Client access to the Internet for the first time need to load the use brush face to obtain temporary IP login module, the customer the opportunity to apply to the ministry under the DHCP server for temporary IP address, will face after the temporary IP address data and compare the face recognition database information, and if the employees in other departments, the server returns an ACK confirmation message, After receiving the ACK confirmation message, the client can use this temporary IP to communicate within the range. If in administration and technical staff, the server will return a digital token, the client sends the digital token of data flow to obtain the DHCP server application for the temporary IP, DHCP server after processing the application, assigned to the client IP formal at the same time, the client before get temporary IP instead of binding, And this mapping relationship will be placed on the relevant router device or storage device, so that the administrative department or technical department personnel to access the external network to do mapping use. The flow chart is shown in Figure 2.

For employees working in other areas and belonging to the administrative and technical departments, it is required to install dual network adapters (with both temporary IP and official IP) as a transition between the enterprise external network and the enterprise internal network.

The significance of this module is as follows: (1) According to the situation of obtaining IP, the attendance of employees can be checked (2) The IP address segments of

departments with different communication security levels can be isolated to improve the security of the network system.

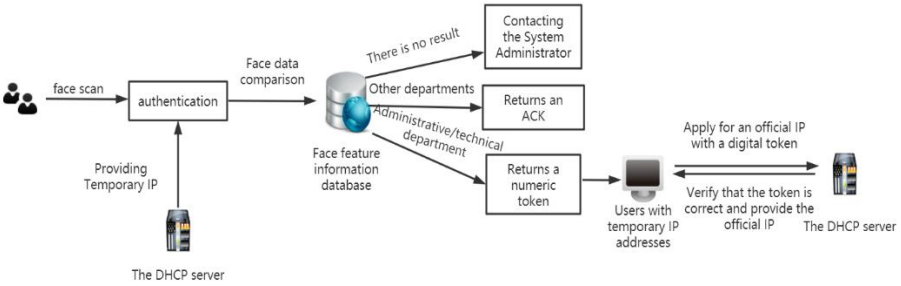

Fig. 2. Obtaining the IP module

5.2 Employee Access to the Extranet module design

From the perspective of enterprise traffic security, devices such as AC, AF, and AD are deployed at the exit from the enterprise network to the extranet. Network administrators can audit all traffic content of the enterprise through the AC [12].

From the enterprise network security considerations, to design a temporary IP users (the user) of other departments only through NAT technology to do a mapping transformation to foreign network access, formal IP user, before the Internet needs to be officially IP mapping to temporary IP, again by temporary IP to access the network through NAT, through the two layers of mapping relation to ensure safety, As shown in figure 3.

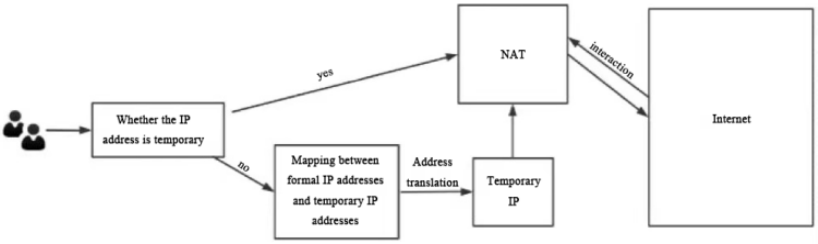

Fig. 3. Accessing the extranet module

6 Key technologies used to design the functionality

6.1 Vlan division technology

VLAN (virtual local area Network) is a network technology that logically groups data interacting within an enterprise based on systems, services, and applications. In the enterprise network project, vlans can be divided into different secondary departments under the same department according to specific requirements. By dividing vlans, a large

broadcast domain is divided into several smaller broadcast domains, so that the subordinates of each department do not affect each other and do not conflict with each other. From the point of view of protocol, the broadcast storm problem of the network is solved, so as to avoid network paralysis and improve the network security performance to the greatest extent.

6.2 The STP technology

STP technology is mostly used in the redundancy between switches, in this design, in order to ensure that the core switch
in the case of redundancy does not occur loop, in the core switching area, using MSTP multi-spanning tree protocol, through the use of examples in the network system to distinguish different layer 2 network system. Within each specific department, we will use RSTP to speed up convergence. In addition, from the perspective of enterprise security, we plan to set up sticky MAC address technology on each switch, and limit the maximum number of connections. In the case of private connection and multiple connection, the switch will initiate a penalty measure, which will punish the content of automatic power outage.

6.3 OSPF technology

OSPF is used between departments. It has the advantages of fast convergence of route changes, no routing loops, VLSM support, and hierarchical area division. When OSPF is used on an enterprise LAN, the route entries on the Intranet are calculated and generated by OSPF without manual configuration by the network administrator. When the network topology changes, the Intranet automatically counts the error points and corrects the route results. OSPF facilitates network management on the Intranet to a large extent.

The internal network of an enterprise is set as Area 0 of the OSPF domain to collect the data flow entries collected by each department, facilitate network management and operation, and create conditions for a high-speed enterprise LAN.

6.4 The ACL technology

An advanced ACL is configured on the core switch to prevent communication between the temporary IP network segment and the official IP network segment, to prevent employees with temporary IP from accessing some ports on the server within the executive department, and to allow only hosts with official IP addresses to connect to the server during a specified period of time. At the same time, change the ACL policy of the firewall to deny all, and open some ports according to the requirements of the enterprise to allow normal service data.

6.5 NAT technology

On the outside of the enterprise network and interaction of the firewall Settings of NAPT, ensure that users interact with the network information security, at the same time, the public network address interface range of rich in the agreement, to ensure that the user's Internet speed stop by address IP pool enough enterprise Intranet users take the network IP address each other shocks caused by network problems. In terms of funding for building an enterprise network, NAT also reduces the cost of applying for public IP addresses.

6.6 DHCP Dynamic address assignment technology

Adopt the way of DHCP allows client dynamically obtain IP addresses, in this design, can according to user's application of IP address as a reference of company attendance, would set the DHCP server Settings on each department core switches, each distribution of DHCP server all the IP address of the unit under the department, Considering the mobile office and other problems, the DHCP server in each department will set a certain amount of temporary IP address segment and formal IP address segment in the address pool. This design also meets the requirement that the heads of other departments (subordinate administrative departments or technical departments) can use the official IP addresses to communicate with each other on the Intranet.

7 Conclusions

With the continuous development of science and technology, more and more technologies from other fields will be integrated into network systems to strengthen the security of network systems or expand various functions. This paper is from the enterprise network security and functional consideration, the face recognition technology into the enterprise network to increase the security of the network system a concept, so as to increase the basic security of the network system. In this paper, the author provides a way of thinking of transforming the results of face recognition technology into different levels of IP so as to integrate it into the network system, and analyzes and summarizes the implementation process of this way of thinking from the point of view of protocol. I hope it can contribute to the security of enterprise network system and the realization of this technology integration in the future.

References

1. C Lin, ZF QIU. Design and Implementation of a Network Multi-Link Backup Technology [J]. Network Security and Informatization, no.6, pp. 73-76, 2022.
2. XX Zhuang.Small and medium-sized enterprise internal network construction research [J]. Journal of electronic test, no.1, pp. 79-80, 2017.

3. JJ Ma, HN Hang. Network Security Design and Application Technology of Small and medium-sized Enterprise LAN [J]. Network Security Technology and Application, no.2, pp. 63-65, 2006.
4. J Juan. Deployment and implementation of firewall in LAN [J]. Science & Technology Innovation and Application, no.22, pp. 109, 2015.
5. H ZHOU. How to use NAT technology to realize LAN user access to the Internet[J]. China Data Communication, no.2, pp. 115-117, 2002.
6. JH LI. Research on Enterprise LAN Building Strategy [D]. Northeast Petroleum University,2011.
7. C E Perkins, E M Belding-Royer, Das S. Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol[S]. IETF. pp.56-63. 2002.
8. V. Taylor, M. Faulkner. Line Monitoring and Fault Location Using Spread Spectrum on Power Line Carrier. IEEE Transmission and Distrbution, no.143, pp. 427-434, 1996.
9. LY Zhang, XH Zhang, Juan Wang. Intelligent Household Network System Design Based on Power Line Carrier Communication[C]. ISTM. pp. 56-63,2007.
10. HH Jin. Design of zigbee-based wireless sensor network nodes and research on their communication [D]. Hefei University of Technology, pp. 56-63,2007.
11. Q Wang. ZigBee-based multi-sensor IoT wireless monitoring system [J]. Electronic Fabrication, pp. 15-23,2017.
12. Y Li, NM Ge, J Chen. Design of ZigBee-based multi-sensor IoT wireless monitoring system[J]. Automation Technology and Applications, pp.56-63, 2015.