Open VPN Application Under Campus Network

Zhengchun Zhou*, and Tongcheng Huang
College of Information Engineering, Shaoyang University, Shaoyang 422000, China

*Corresponding author: 20156@hnsyu.edu.cn

Abstract. For security and intellectual copyright considerations, colleges and universities generally have the same problem: non-campus residents cannot access many resources on the campus network. OpenVPN is an open source based on the SSL protocol, combined with the actual needs of campus network applications, it describes in detail how to use the open source OpenVPN technology on the LINUX operating platform to build a user access system. Users can quickly access campus resources by establishing a connection with the OpenVPN server through the client program. Without additional investment, the confidentiality of data is ensured. It allows users to break through the limitations of time and space, which not only facilitates users, but also improves the utilization rate of campus network information resources.

Keywords: Keywords: OpenVPN, campus network, campus resources, remote access.

1. Introduction

VPN is a technology that uses tunnel technology, encryption, and identity authentication to establish a private network on a shared network. It is called a virtual network mainly because the connection between any two nodes of the entire VPN network does not have the point-to-point physical link required for the construction of a traditional private network, but is based on a public network service provider ISP. Logical network on top of the network platform. The user's data is transmitted through a logical tunnel established by the ISP in the public network, that is, a point-to-point virtual private line. Through the corresponding encryption and authentication technology to ensure that the user's internal network data is safely transmitted on the public network, so as to truly realize the exclusiveness of the network data. Applying VPN technology to the campus network can break through the regional restrictions of the campus private network, optimize the management and application of the campus network, and meet the requirements of teachers and students to access campus network resources outside the campus. Teachers, students and employees can use the system to enter the campus network and access as internal users of the campus network [1]. In response to the actual needs of campus network security, this article proposes a VPN protocol selection and design plan suitable for medium-scale campus networks, and completes the implementation of OpenVPN combined with firewalls.

2. OpenVPN technology principle

OpenVPN software integrates multiple technologies such as virtual network card equipment, TCP/IP network technology, routing technology, and SSL data transmission encryption, allowing both parties involved in establishing a VPN connection to use a pre-shared private key, a third-party digital...
certificate or a username/password for identity verification, the software uses the SSL V3/TLS V1 protocol, uses a large number of OpenSSL encryption libraries, and can use TLS/SSL encryption to ensure the security of data transmission. The core of OpenVPN technology is a virtual network card. Virtual network card is the key to OpenVPN's SSL VPN function. It uses TUN/TAP driver to provide two types of general TUN/TAP virtual network interfaces, which support routing and bridging modes respectively. The OpenVPN driver part realizes the network card processing and character device. Using the network card driver to process network data, it can receive data packets from the TCP/IP protocol stack and send or pass the received data packets to the protocol stack for processing; use the character device to complete and apply the data interaction of the layer realizes the transmission of data packets between the kernel and the user space, and simulates the data reception and transmission of the physical link. During the use of OpenVPN, the routing table must be modified. When a remote user connects to the OpenVPN service program, the application sends data, and the system sends the data to the virtual network card through the routing mechanism. The character device reads the data and sends it to the application layer [2]. Finally, the physical network card completes the data transmission; OpenVPN service program the data can be received through the physical network card, and the character device transmits the data to the virtual network card, and finally the data is transmitted to the upper application through the network stack. Figure 1 shows the schematic diagram of the data transmission between the client and the server and the logical relationship of each level. It can be seen from the figure that OpenVPN provides two types of virtual network cards, TUN and TAP. TUN is used for virtual three-layer network, and TAP is used for virtual two-layer network. The logical channel between virtual network cards connects the client and server. And establish SSL/TLS connection in the network transmission layer.

3. Design of campus network VPN system

3.1. Design ideas
As shown in Figure 2, suppose that the internal server address segment of the campus network is: 192.168.1.0/24, the OpenVPN server has a legal IP address connected to the Internet, and public network users establish a connection with the Internet. An encrypted connection tunnel is established with the OpenVPN server through the OpenVPN client software to access the application server protected by the OpenVPN server in the local area network.
In the campus VPN network system structure, a server in the main campus network is used as a VPN server, a server in the branch campus network is used as a VPN client, and other remote mobile users outside the campus are also used as VPN clients. The VPN server in the main campus has an IP in the campus LAN and an IP connected to the external network; remote mobile users outside the campus can access the Internet through dial-up, ADSL, etc., with a static or dynamic IP; in the branch campus The VPN client acts as a server in the local area network of the campus [3]. It has an internal IP and an external IP. Other machines on the campus network connect to the server to use the VPN tunnel service.

To make the current VPN network available, a series of configurations are required. Use OpenVPN software to configure SSL in two security modes, namely static key method, RSA certificate and key method based on the use of SSL/TLS protocol. The former is simple to configure, does not need to maintain key certificates, but limits the number of users, only supports one-to-one connections, and the client must pre-deploy a static key, which is not sufficiently secure; the latter guarantees security, but requires the additional maintenance of the key certificate is more complicated than the former configuration. In the actual use environment, RSA certificates and keys are generally used for security authentication.

3.2. Overall design
In order to realize the safe and stable remote management and maintenance of the campus network by the administrator on the external network, it is necessary to appropriately improve the original campus network system topology. Figure 3 is the original campus network management structure, and Figure 4 is the system structure of the design scheme for remote management and maintenance of the external network. It can be seen that an OpenVPN server has been added to the campus network and the corresponding authority configuration has been carried out. Configure the access authority of the OpenVPN server in the campus network core and convergence layer switches, and authorize the access to the network management server to realize the network management function. At the same time, the routing table is updated so that the data packets sent from the network management server to the OpenVPN client with the target address are forwarded to the OpenVPN server for processing, and the data packets are then forwarded by the OpenVPN server to the OpenVPN client [4]. In addition, access control lists need to be set up in the campus network core and convergence layer switches to authorize and isolate the permissions of the OpenVPN client to ensure security requirements.
Figure 3. The original campus network management structure diagram

Figure 4. The system structure diagram to realize the remote management and maintenance design of the external network

Compared with the original network management structure, this design achieves the following functions: 1) The administrator can connect to the OpenVPN server through the external network to remotely obtain the IP address segment determined by the campus network; 2) In order to ensure the security of the network, the network connection and data During transmission, the data is encrypted; 3) The campus IP address segment dedicated to remote management is allocated and isolated from the original management IP address segment in the school to ensure security.

3.3. Management and client program development

Although OpenVPN is very powerful, there is no better management software, especially the management software that can run under the Windows operating system, which is completely blank. Although the client software has open source OpenVPN, for new users, there are certain problems with the use of certificates and the configuration of the client. In response to the above problems, we have developed corresponding management and client systems. This system relies on the school’s digital library and the Scientific Research Information Network of the School of Computer Science of Chongqing University of Posts and Telecommunications (hereinafter referred to as: Scientific Research Information Network). The user profile information uses the data of the Scientific Research
Information Network [5]. User registration, certificate application, password retrieval and other related work on the scientific research information network.

3.3.1. User authentication module. In terms of user verification, although OpenVPN has a strong certificate verification function, there are greater risks in the issuance and transmission of certificates. Once the certificate is stolen, illegal users can intrude into the school intranet. For security, our school adopts a combination of username/password verification and certificate verification. Because OpenVPN does not provide a specific user name and password to verify the mechanism, the author and colleagues developed a verification program vpn_pasw in C++, which will be automatically called when the user accesses and authenticate the user [6]. The verification program mainly involves User data information is shown in Table 1.

| Field       | Attributes | Description            |
|-------------|------------|------------------------|
| User_name   | string     | username               |
| User_pass   | string     | password               |
| User_active | bool       | Is online              |
| User_right  | int        | User rights            |
| User_offtime| int        | User temporarily away time |

User_active defines whether the user is online to prevent multiple users from logging in with the same account. User_right defines two user rights, mainly to distinguish between users and administrators. User_offtime defines the time for the user to leave, and is set to automatically disconnect the user 15 minutes after leaving.

3.3.2. User monitoring module. Remote access involves the security of the campus network, so the users who access it must be monitored. This system has designed a connection module vpn_conn and a disconnection module vpn_disn, which are called when the user accesses and disconnects. vpn_conn mainly obtains user access time, location, port, protocol and other information and stores this information in the database. When disconnected, vpn_disn is called to obtain disconnection time, traffic and other information to achieve traffic analysis and connection statistics. Features [7]. Part of the data information used to realize this function is shown in Table 2.

| Field       | Attributes     | Description         |
|-------------|----------------|---------------------|
| starting_time| time           | Connection time     |
| trusted_ip  | string         | Real IP             |
| trusted_port| int            | Port for connection |
| protocol    | string         | Protocol used       |
| remote_ip   | string         | Login IP            |
| bytes_received| double        | Downstream traffic  |
| end_time    | time           | Exit time           |

3.3.3. Management module. The management module is written in php, and the VPN management and "My VPN" options are added to the original scientific research information network to display and process VPN-related data. Only the administrator has the right to enter the VPN management item. In this project, the administrator can Perfrom operations such as issuing certificates, revoking user certificates, deleting illegal users, viewing and modifying basic user information. In the "My VPN"
option, users can log in with the research information network account to view their personal information and apply for certificate information.

4. Conclusions
Through the problem analysis, theoretical research, and system design of the actual problems that the network administrators are outside the campus in the campus network management process, the actual application system to solve this problem is built based on the OpenVPN technology, and finally put into the campus network Manage running and testing in the actual environment. The system runs stably and the application effect is good, which proves the feasibility and practicability of the system design, and the results of this research can be promoted and used in various similar situations, which has high practical application value.

Acknowledgments
This dissertation is supported by Scientific Research Project of Hunan Provincial Department of Education (Research on virtual private network based on openvpn technology. Grant No:20C1686).

References
[1] Doriguzzi-Corin, R., Scott-Hayward, S., Siracusa, D., Savi, M., & Salvadori, E. Dynamic and application-aware provisioning of chained virtual security network functions. IEEE Transactions on Network and Service Management, 17(1) (2019) 294-307.
[2] Muñoz, R., Vilalta, R., Casellas, R., Martínez, R., Szyrkowice, T., Autenrieth, A., & López, D. Integrated SDN/NFV management and orchestration architecture for dynamic deployment of virtual SDN control instances for virtual tenant networks. Journal of Optical Communications and Networking, 7(11) (2015) 62-70.
[3] Tian, R., & Zhu, H. Complex application identification and private network mining algorithm based on traffic-aware model in large-scale networks. Peer-to-Peer Networking and Applications, 12(6) (2019) 1594-1605.
[4] Tsai, P. W., Cheng, P. W., Chou, H. Y., Luo, M. Y., & Yang, C. S. Toward inter-connection on OpenFlow research networks. Proceedings of the Asia-Pacific Advanced Network, 36(7) (2013) 9-16.
[5] Alghamdi, T. M. Throughput analysis of IEEE WLAN ‘802.11 ac’ Under WEP WPA and WPA2 security protocols. Int. J. Comput. Netw., 9(1) (2019) 1-13.
[6] Erazo, M. A., & Liu, J. A model-driven emulation approach to large-scale TCP performance evaluation. International Journal of Communication Networks and Distributed Systems, 5(1) (2010) 130-150.
[7] Kanchanasut, K., Tunpan, A., Awal, M. A., Das, D. K., Wongsawardsakul, T., & Tsuchimoto, Y. DUMBONET: a multimedia communication system for collaborative emergency response operations in disaster-affected areas. International Journal of Emergency Management, 4(4) (2007) 670-681.