Design of Border Security Defense System for VPN Network in Power Enterprises

Ma WenZhen*, Xu MingChang
State Grid NingXia Wuzhong Electric Power Company Information & Telecomunication Branch (Data Center), WuZhong, NingXia
'E-mail: dec0615@163.com

Abstract: In order to ensure the safe and stable operation of the power system, the VPN network border security defense system of power enterprises is designed. The hardware of the system is planned and designed, including cooperative intrusion detection, security audit, cooperative camouflage, collaborative firewall, disaster recovery and electronic forensics. On the basis of the hardware design, the network data in the gateway is detected by using the cooperative control framework and other security technologies, and the attack behavior is analyzed by using host based intrusion detection, and the network information security situation assessment based on si-s0 is proposed. The algorithm estimates the security state of network intrusion information and realizes the security defense of network boundary. The experimental results show that the designed VPN border security defense system has higher security than the traditional system, and fully meets the research requirements.

1. INTRODUCTION
With the continuous progress of information and knowledge technology in China and the popularization of electronic network, computer network technology has developed rapidly in China. At the same time, enterprises are making more and more use of network information technology, among which electric power enterprises are one of the important users of enterprise network technology[1-2]. In order to prevent power grid accidents caused by large-scale power outage and information security, and to avoid the loss of users and the leakage of business secrets or sensitive information, this paper proposes and designs a VPN network border security defense system of power enterprises. Through the analysis of the current situation of enterprise information security, it is clear that the information security threats faced by enterprises, and take corresponding management measures and technical means, which can effectively prevent To prevent the occurrence of enterprise information security accidents, ensure the security of enterprise information system and the safety of users on the power grid related business system and data processing, ensure the safe access of information network, and control the network information security risk.

2. POWER ENTERPRISE VPN NETWORK BORDER SECURITY DEFENSE SYSTEM

2.1 system hardware configuration
Aiming at many problems existing in collaborative defense of electric power enterprises, a collaborative defense system for border security of VPN network of electric power enterprises based on kernel identification, FIFO and ID generation technology is designed [3]. As far as the power enterprise VPN network is concerned, when the computer receives a large amount of data information about the
network behavior, a number of RAM sub-bodies will be generated at the boundary of the VPN network, one of which will enter the system receiving module through the transmission channel, and the other will directly receive the RAM sub-body through the ID sub-body to ensure the subsequent security identification operation. Based on this, the VPN network security architecture of the power supply company is optimized as follows:

Generally speaking, the network collaborative security system can be divided into six sub-security systems: collaborative intrusion detection, powerful security audit, collaborative camouflage, collaborative firewall, disaster recovery and electronic forensics. Graph logic control represents the cooperative logic control relationship in the strong security audit system, and logic control represents the logic control relationship when the strong security audit system is not started. There are two levels of cooperation[4]. The subsystem is protected by cooperative control framework. Taking dm9000 Ethernet card as the main control chip, the design of the whole hardware structure has the characteristics of low cost and high performance. The overall hardware framework is shown in Figure 2.

![Network boundary security protection architecture](image-url)
2.2 Network Information Security Status Assessment

At present, the information network of electric power enterprises in China mainly adopts the mode of "vertical direct connection and horizontal series connection". Provincial power grid companies directly connect with the State Grid to realize vertical direct connection, and local municipal power grids also adopt the "horizontal series" mode. Effectively protect internal and external networks[5]. In the Windows operating system, as long as the system resources are associated, the system will send a request to the system in a specific way, and then the operating system will execute the request. The importance of system call depends on the hardware structure of CPU, and the system call running in the core space is the core communication means that all processes must use[6]. Therefore, in order to achieve illegal purposes, illegal attackers must access system resources through illegal system calls, that is to say, by judging whether the system calls are legal, they can intercept illegal attacks in real time and realize interception and other responses. It is divided into basic function monitoring module and application evaluation module to realize system application development. The hierarchical optimization structure of system application is shown in Figure 3

![Figure 3 System application level optimization](image)

The designed active defense system makes up for the deficiency that power enterprises only have two product functions: host active defense and network active defense, and can protect PC terminals more comprehensively. This system adopts NIPS first-class protection to detect the network packets of the protected PC terminal flow, and handle the problems in time when they are found; HIPS provides system security protection and file security protection[7]. In the stand-alone system, cooperative control framework and other security technologies are adopted to realize the security of the stand-alone system, detect the network data in the gateway, and use host-based intrusion detection to analyze the attack behavior. After detecting the attack, IDS will send a notice to the audit system. If there is a
strong audit system, the audit system will evaluate the existing security based on the comprehensive audit results.

Intrusion information and security information are divided into left and right subsets U (intrusion information) and N (security new information), in which intrusion information has the strongest dependence on security new information set\[8\]. The common features of left and right subsets are searched from bottom to top, and the complexity of dimensionless information filtering is reduced by iteration. On this basis, this paper proposes a network information security situation estimation algorithm based on si-s0, which sets the estimated value of network information security situation as s0, sets the characteristic value of capture factor behavior as si-s0, defines the data security on network information sequence t as s0 (T), T=1,2,3, … n, and then sets the characteristic value of the estimated value of network intrusion information state as follows:

$$S_i(t') = [S_i(1), S_i(2), ..., S_i(n)]$$  (1)

Set t for information detection time, p for intrusion information measurement, n for object number and other uncertain values. Then the correlation coefficient of sequence Si and S0 at point t can be defined as:

$$\delta_{i}(t) = \frac{\min \min |S_i(t) - S_i(p)| + \mu \max \max |S_i(t) + S_i(p)|}{|S_i(t) + S_i(p)| + \mu \max \max |S_i(t) - S_i(p)|}$$  (2)

If u is the evaluation value of possible intrusion attacks during network operation, k is the network operation time, and a is the amount of intrusion information provided by network structure. Intrusion information refers to the degree of network security attacks caused by collecting and processing bad network information in the big data environment. The algorithm is as follows:

$$\delta(S_0, S_i) = \frac{1}{t \sum \mu_{0}(t), \mu \in (0,1)}$$  (3)

Through the comprehensive analysis of the above formulas, the preliminary evaluation algorithm of the security situation evaluation index of network R affected by intrusion information in the primary industry is obtained:

$$R_{S_i}(t) = \delta(S_0, S_i) \sum_{i=1}^{t} 10^{a_0} \nu$$  (4)

In the above algorithm, the amount of information that can be provided in the security defense system is v. Combined with the above algorithm, the characteristics of intrusion information security risk in cloud computing network are extracted, and the evaluation of network information security status is completed\[9-10\].

2.3 Realization of network border security defense
According to the standardized quantitative processing scheme, users are divided into three levels: access, access users, access and users. Access refers to remote receiving network services and data interaction. For a topic, all accesses to objects are a collection. Authorized by the administrator, the user represents the user right with independent space and resources; Root means that the host can control all resources. Because the partial order distribution of Access< User< Root satisfies the three-tier relationship, they can correspond to different hosts one by one. The connection relationship between hosts is the starting point of host connection. The original host connection can reach the original host, but there is no connection between the original host and ordinary host. The collected modeling information needs to be analyzed in detail. A data string \{a, b, IP, TCP, HTTP\} can be expressed as: a sends IP data to b, and a provides HTTP service for b. IP protocol (Network Collections protocol), which defines IP packet format, is used to complete grouping and reorganize grouping.

As an important part of network border security defense, ICMP protocol provides an important service mode, which tests the target status and accessibility of messages in detail, controls packet flow,
and carefully checks circular routes or long routes. The main function of TCP protocol transport layer is to establish reliable section connections, and effectively provide users with virtual circuits and data flow-oriented transmission services. UDP protocol provides a protocol port to distinguish multiple programs running on the same computer. On the other hand, it is unreliable. This service neither acknowledges the arrival of messages, nor sorts messages, nor controls traffic. IP is transmission control protocol or internet protocol. TCP/IP is the most basic protocol on the internet, which includes TCP and bottom IP. Because Terminal Control Protocol (TCP), Hypertext Transfer Protocol (HTTP) and Network Interconnection Protocol (IP) limit the linked list to the hierarchical connection relationship of the protocol stack, only a group of changes in the database can be stored in the linked list, thus reducing the vulnerability to attacks. Chain PT is used to store a set of individual changes, based on which the network security protocol chain structure is optimized as follows:

In the VPN linked list, the P node mathematically models the state information of the VPN network security assessment, which can be expressed as (ip, r). On the basis of mathematical modeling, firewall filtering and packet intrusion detection rules are further set to make the published network packets completely inaccessible to related network applications; initialize the active defense part of the host and create device objects. The created access rules will be stored in the rule base and memory. Monitor all system calls related to protected resources, check their effectiveness according to established rules, and finally decide whether to publish or request user feedback. Based on the principle of active defense, a mathematical model of virtual private network security evaluation is established, and the virtual private network model is used to evaluate the whole active defense network. The vulnerable network behavior of active defense virtual private network is simulated and analyzed. According to the required security information, we can find a variety of possible active defense security combination attack methods. Without LAN security assessment, virtual private network can not be effectively active defense. On this basis, by collecting the data related to the network security attributes in the active defense system, combined with the analysis of the network data structure and storage space, the attack scenario model of the active defense system is established, and the local evaluation results are obtained. The security evaluation method of active defense network in virtual private network (VPN) is proposed by using correlation matrix analysis method.

3. ANALYSIS OF EXPERIMENTAL RESULTS

In order to verify the practical application effect of VPN network border security defense system in power enterprises, comparative detection experiments are carried out. In order to ensure the experimental effect, the experimental parameters are set uniformly.

It is assumed that the evaluated target mobile network contains seven hosts, and the network also requires relatively low confidentiality, integrity and availability. The first and fifth hosts contain important data, and they are set as follows:

\[
q_i (1), q_i (2), \ldots, q_i (7) = (0.5, 0.25, 0.25, 0.1, 0.1, 0.1, 0.25) \]

\[
q_i (1), q_i (2), \ldots, q_i (7) = (0.25, 0.1, 0.1, 0.1, 0.25, 0.1, 0.1) \]

\[
q_i (1), q_i (2), \ldots, q_i (7) = (0.2, 0.1, 0.1, 0.1, 0.3, 0.1, 0.1) \]

\[
q_i (1), q_i (2), \ldots, q_i (7) = (0.1, 0.1, 0.4, 0.1, 0.1, 0.1, 0.1) \]

(5)
Combined with the above algorithm, the operation effect of the traditional method and the method in this paper is compared, and the detection results are recorded as follows:

![Comparison test results](image_url)

**Figure 5 Comparison test results**

Based on the above detection results, it is not difficult to find that, compared with the traditional method, the detection error of dangerous data in the actual application process of the VPN network border security defense system designed in this paper is significantly lower, which proves that the power system under this method has a better effect in the actual application process, and can more effectively guarantee the development of power enterprises.

4. **CONCLUSION**

With the rapid development of network technology and multimedia information technology, people's understanding of network technology is more and more in-depth. The network information system of power grid enterprises initially realizes the exchange and transaction between network resources and network users, which facilitates people's life. However, the network information risk and the application of specialized network information security technology have become the main obstacles to the normal operation and development of the network information system of power enterprises, and also bring hidden dangers for its safe and stable operation. In this regard, power enterprises should make special preparations for network security technology, deal with various problems and risks existing in its network information system, ensure its normal operation, so as to promote the progress and development of network information technology in power enterprises, and provide powerful guarantee for network information security of power enterprises.

**REFERENCE**

[1] Muhanji S O, Schoonenberg W C H, Farid A M. Transforming the Grid's Architecture: Enterprise Control, the Energy Internet of Things, and Heterofunctional Graph Theory[J]. IEEE Power and Energy Magazine, 2019, 17(5):71-81.

[2] Galtseva O, Bordunov S, Zhiganov A, et al. Technology of Gold-Containing Technogenic Raw Materials Processing Using the Electric Explosion Method[J]. Materials Science Forum, 2019, 942(12):30-39.

[3] Liu J, Fu X, Xu F, et al. Partner selection for state-owned power grid enterprises in China based on an extended TODIM method: A case study in Inner Mongolia[J]. Intelligent Decision Technologies, 2018, 12(4):1-12.

[4] Kolomiets Y G, Menshikov Y A, Tarasenko A B. Influence of Insulation Level on Electric Power Quality and Transformation Efficiency of Grid-Connected Photovoltaic Power Plants[J]. Applied Solar Energy, 2018, 54(4):246-250.
[5] Shah D. Chatterjee S. A comprehensive review on day’ head electricity market and important features of world's major electric power exchanges[J]. International Transactions on Electrical Energy Systems, 2020(3).

[6] Zhang Y, Wang L, Meng L. An Analytical AC Resistance Calculation Method for Multiple-Conductor Feeder Cables in Aircraft Electric Power Systems[J]. IEEE Transactions on Industrial Electronics, 2020, 67(5):3340-3349.

[7] Martinez-Parrales R, Fuerte-Esquivel C R. A new unified approach for the state estimation and bad data analysis of electric power transmission systems with multi-terminal VSC-based HVDC networks[J]. Electric power systems research, 2018, 160(jul.):251-260.

[8] Gaynanov D A, Kashirina E S, Khabirova Y F. On an Effective Ratio of Conventional to Renewable Energy Sources in the Russian Electric-Power Industry[J]. Russian Electrical Engineering, 2018, 89(1):9-12.

[9] Hayes J G, Goodarzi G A. Book review: Electric Powertrain: Energy Systems, Power Electronics and Drives for Hybrid, Electric and Fuel Cell Vehicles[J]. IEEE Aerospace and Electronic Systems Magazine, 2019, 34(2):46-47.

[10] Li Y, Huang G Q, Wang C Z, et al. Analysis framework of network security situational awareness and comparison of implementation methods[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 2019(1).