Research on the Development Trend of Enterprise Information Security Strategy in Cloud Environment

Kai Li(✉), Kai Li, Chunlei Chang, and Qiaoli Wang

State Grid Xinjiang Electric Power Co., LTD. Information Communication Company, Urumqi 830000, Xinjiang, China
2438396213@qq.com

Abstract. Due to the combination of cloud computing and big data, the infrastructure and architecture of information networks and information systems have changed. Defense centered strategies cannot cope with advanced target attacks. By analyzing the security requirements of the bank's digital transformation, guided by the concept of "zhongtaihua", this paper designs the security middle platform solution, studies the construction technology of the security service function chain required by the construction of the security middle platform, and proposes the example selection and routing optimization algorithm of the security service function chain, which provides a reference for the security capacity construction of the bank in the process of digital transformation.

Keywords: cloud security · Information security architecture · Safety Center · Service function chain

1 Introduction

At present, the technology based on the above cloud security architecture is also relatively mature in the industry. With the rapid development and application of various cloud computing forms such as public cloud, private cloud and hybrid cloud, cloud security technology has also been widely used and practiced. A typical cloud security technology architecture is shown in Fig. 1.

The current typical cloud security technology system mainly includes three aspects: cloud platform basic security, cloud tenant business security and cloud security services. The specific security capabilities of cloud platform and cloud tenant cover network security, host security, application security and data security.

1.1 Enterprise Data Security Status in Cloud Environment

In recent years, with the rapid development of Internet of things, cloud storage, cloud computing and other new technologies, data information has shown an explosive growth trend. Through the analysis of these information, it can effectively help enterprises grasp

G. Guan et al. (Eds.): ICBDSS 2022, AHCS 8, pp. 205–212, 2023.
https://doi.org/10.2991/978-94-6463-064-0_24

the market background, perceive the industry direction, and formulate better business strategies for enterprise development direction and risk prevention and control. More and more enterprise operators begin to pay attention to the business value of "big data", and regard valuable enterprise data as the "golden key" for enterprises to win market opportunities [1].

In the era of big data, enterprises are accumulating risks while acquiring the information value of cloud platforms. First, viruses and Trojans invade the enterprise private cloud. Big data is uploaded, downloaded and exchanged in the cloud, which makes the cloud platform vulnerable to hackers. Once the cloud platform is invaded and data is leaked, it will bring immeasurable losses to the enterprise in terms of brand, reputation, research and development, sales, etc. The second is the loss caused by internal employees' illegal theft of enterprise data or negligence, because in the process of work, enterprise employees inevitably need to contact the core data or internal confidential information of the enterprise. Once information disclosure occurs within the enterprise, the information security of the enterprise will be threatened, and its destructive power will far exceed the impact of external disclosure, and even bring ultimate disaster to the enterprise [2].

According to authoritative statistics, in 2013, 81% of enterprise information security disclosure problems were negligent disclosure or active theft by internal personnel. Only 12% of information leakage is caused by external hacker attacks, system vulnerabilities, virus infection and other problems. The loss caused by internal disclosure is 16 times that of hacker attack and 12 times that of virus infection.

To sum up, whether from the perspective of preventing hackers from malicious attacks on data or from the perspective of internal staff security, in order to ensure enterprise information security, there is an urgent need for a more effective method to effectively manage enterprise information security. This method should not only strengthen external prevention in the era of big data, but also achieve effective prevention and control of internal systems. The emergence of data leakage prevention technology has better realized the "internal and external prevention" of enterprise information security.

"Data leakage prevention" technology, also known as "data leakage prevention", encrypts and protects documents through efficient and secure dynamic encryption and decryption technology, thus playing the role of data leakage prevention for enterprise information security [3]. All kinds of data and files protected by "data leakage prevention" can completely prevent internal files from being illegally copied, browsed, stolen and photographed. Any operation of all users is constrained and monitored by security management rules, so information security in the enterprise is no longer a problem.

Nowadays, data information has become an important strategic resource for enterprise development. In order to ensure enterprise information security, it is necessary to formulate corresponding management measures, establish an enterprise information security model in combination with a perfect enterprise information security management system, and enjoy the value enhancement brought by "big data" on the premise of comprehensively ensuring enterprise information security.

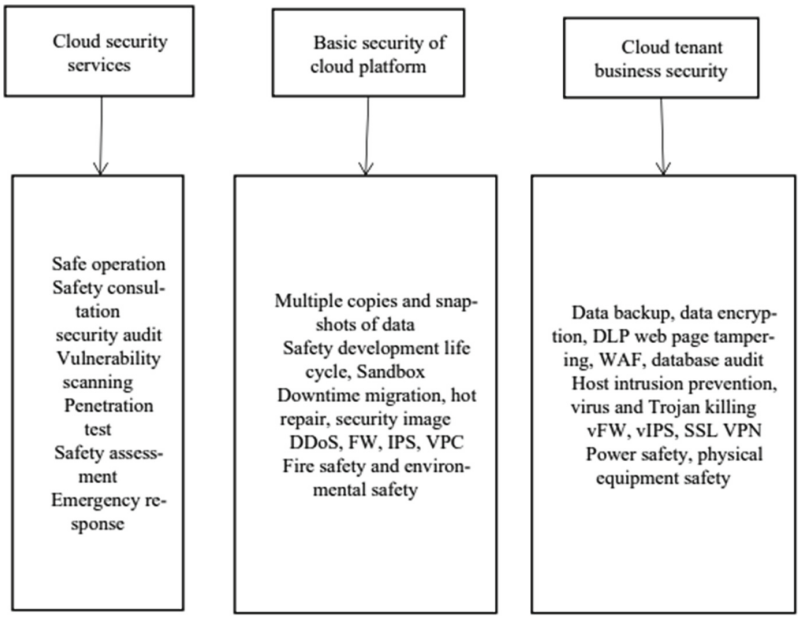

Fig. 1. Typical cloud security technology architecture (Photo credit: Original)

2 Construction Technology of Security Center

The construction of the security center is a continuous work. It needs to build the security center on the basis of the existing security system, but it is faced with such problems as the management of traditional security equipment and the inconsistent data interface. Therefore, the construction of the security center needs to be carried out step by step, from the integration of security capabilities to the arrangement of security capabilities, and the security service function chain should be built as required. Realize the unified management of network security resources in the background. Through the atomic decoupling of capabilities, it has a scene based security ecology that can be scheduled and arranged, and provides service-oriented network security capabilities to the foreground.

2.1 Security Capability Integration

Most enterprises have a certain network security construction foundation, such as meeting the requirements of level 3 protection and deploying situational awareness. Security systems such as Threat Intelligence and intrusion detection have precipitated some security data, but the business scenario is complex, and the requirements for network security are high. Existing security equipment, such as intrusion detection system (IDS), firewall (FW) and deep packet detection system (DPI), are not only poorly configurable and cannot cooperate with each other, but also do not have flexible access methods. Unified API and control standards can be developed for existing security equipment, Form north and South interfaces to realize unified management, policy configuration and security

data collection of equipment of different manufacturers and models. Through the development of unified data and control interfaces, the existing security capabilities can be integrated to a certain extent. However, the development of the control platform requires a large amount of work and requires the cooperation of various security equipment manufacturers, which makes it difficult for technology and management.

2.2 Arrangement of Safety Capability

On the basis of integrating existing security capabilities, with the full cloud of business, virtualization technology can be further used to arrange security capabilities. By combining the security capabilities of different systems or components according to certain logical relationships, service-oriented security capabilities can be provided for the front desk.

Based on Software Defined Network (SDN) and network function Virtualization (nfv) technology, the virtualization security function is realized on the general hardware platform. In the nfv environment, traditional security devices have corresponding virtualized security instances (VSA), such as vids, VFW, vdpi, etc., which are flexible and highly scalable. Users can establish different security policies according to different needs, and arrange the service function chain (SFC) according to different security policies.

2.3 Safety Service Function Chain

The construction of the security service function chain needs to arrange the virtual security capability, schedule the data flow to the corresponding virtual security instance, and provide the corresponding security services according to the user's security requirements.

The important components responsible for security SFC in the security middle platform framework include VSA instance and vswitch. Capability orchestration, policy management, capability management, service management and restful programming interface. Among them, VSA instances are security resources created based on virtualization technology, such as vids, VFW, vdpi, etc. Vswitch is responsible for pulling the traffic to the corresponding security function instance according to the traffic pulling strategy, recovering the instance traffic, and pulling it to the next hop to realize the security function service chain. The capability orchestration component is responsible for security event analysis and dynamic response. When a security attack is found, it generates a security SFC request according to the rules and sends the request to the service management component. Service management is responsible for the creation and management of service directory and service registration load SFC instances. Capability management is responsible for the creation and management of capability directory and capability registration, and security function instances. Policy management is responsible for the management of diversion strategy, policy conflict and traffic traction strategy. Restful programming interface is SFC management pair, which provides restful based programming interface to facilitate integration with other services or applications.

2.3.1 Construction Process of Safety Service Function Chain

The security application layer initiates a customized security service request and sends an SFC request to the service management of the security control layer. Figure 5 shows the security service chain scheduling process. The service management first finds the service chain directory and selects the appropriate SFC. By checking the service chain list, it is determined whether the SFC request is an instance registered and activated in the existing SFC list. If an active instance already exists, reuse the SFC active instance and create a corresponding diversion policy. If the relevant SFC instance is not established, the service management will find the capability directory and select the security capability required by the SFC according to the requirements. Instantiate and deploy the security capability image in the corresponding host through the SDN controller, and register it in the capability management. Finally, create a diversion strategy and a traffic traction strategy, and feed them back to the security management for policy management.

2.3.2 Optimization of Safety Service Function Chain

In order to ensure the implementation effect of security SFC, it is necessary to consider the VSA instance and route selection strategy to make the network flow pass through the corresponding VSA correctly and efficiently. In this paper, we propose a secure SFC instance selection and routing optimization algorithm from the perspectives of instance resource availability and network delay, which improves the actual service quality of secure SFC.

1) Instance selection mechanism.
During SFC implementation, VSA instance and link selection shall be considered to improve resource utilization and SFC service effect. In the process of building a safe SFC, the requirements of the SFC shall be specified. The VSA types and sequences of SFC are represented as v = {V, V2, V,}, where p is the number of VSA types. The priority of VSA is expressed as priority (V;), When SFC is implemented, the traffic route is set from high to low by traversing the priority of each element in the set v.

Similar VSAs often have multiple instances at the same time, and their set can be expressed as $V = \{v_1, v_2, ..., v_p\}$. Where I $\in$ 1, 2, ..., P, $Q_I v_i$ The number of instances of.

The real-time resource utilization rate of a VSA instance 0U is expressed as: ψ_{ij}. Set the utilization threshold of this type of VSA as: δ_i. The VSA instance. Idle degree of ϕ_{ij} The calculation formula of J is:

$$\phi_{ij} = (\psi_{ij} - \delta_i)/\psi_{ij} \tag{1}$$

The VSA instance sequence of the security SFC can be expressed as listsfc, which can be obtained by the execution of algorithm 1 and fed back to the service registration component. Algorithm 1 traverses all types of VSAs and selects instances with low resource utilization to form a security function service chain. For VSAs whose resource occupation exceeds the threshold, the creation mechanism is triggered. According to the example sequence, the SDN controller can conduct traffic traction and scheduling to ensure the normal operation of the safe SFC.

Algorithm 1. Instance selection algorithm.
The input: V, δ, ψ;
The output: $list_{SFC}$
SORTA by priorty (V_i)to listv
/*Specify the VSA type sequence */ required by the SFC
For cach V, in list V /* Indicates the sequence of VSA types traversed */
For each v, in v, /* Traverses instances of the type */
COMPUTE/* Computes the instance of this type free
Case * |
end for

2) Routing mechanism

The instance selection mechanism only selects the instances that provide services according to the idle resources of the VSA instance, and does not consider the network delay problem. In the data center with good network conditions, the effect of the example selection algorithm is better, but in the multi cloud environment, the network delay will seriously affect the quality of service. Therefore, in the case of investigating the utilization rate of VSA resources, the network delay should also be analyzed and evaluated, and the VSA instance sequence with the best overall service should be given.

The type sequence listv may be formed according to the priority of the VSA type. If each type of VSA instance is regarded as a vertex and the network delay between the instances is regarded as a path weight, the problem of selecting the VSA instance sequence with the smallest network delay becomes a minimum path problem. The minimum path algorithm can be used to traverse all VSA sequences and select the smallest network delay sequence. However, this method traverses many invalid sequences and does not consider the utilization of instance resources.

Therefore, the VSA instance sequence of the secure SFC can be modified by considering the network delay problem based on the algorithm 1. V; The network delay between and V can be expressed as delay; Set the network delay threshold delay. If the delay is greater than the threshold value, the quality of service will be seriously affected, and the route will be discarded.

First, based on the sequence listsec output by algorithm 1, the network delay threshold is set, the traffic path is traversed, and the route with large delay is replaced, and the list SC is partially modified.

Algorithm 2. Route optimization algorithm
The input: $list_{sfc}$ V;
The output: $list_{SFC}$
FOR EACH V in $list_{sfc}$
/*Specify the VSA type sequence */
DETECTION and COMPUTE delay
/* Indicates the sequence of VSA types traversed */
IF $DElay_{iy} \geq DElay$ then for each v, in v,
/* Traverses instances of the type */
SELECT the minimun of Delay +Delay
/* Computes the instance of this type freeCase * |
REPLACE in $list_{sfc}$

/* Replace instance * |
end for

3 Safety Analysis of Safety Center

The security center not only improves the efficiency of the bank's security capacity building, but also brings new security risks.

1) Data security

The security center realizes the standardization and centralization of security data. Through the security center, various sensitive security data can be accessed, including host operation data, security equipment logs and traffic data. The security center is faced with great data security risks. Data centralization brings about risk centralization and hazard expansion.

In the construction and operation of the security center: unified security authentication and permission management shall be established, and the access to data shall be controlled in a fine-grained manner by dividing the permission levels; Data classification and hierarchical management shall be established, and different safety protection measures shall be taken according to the safety level of the collected data; A data mobility monitoring mechanism shall be established to sense the data operation behavior of users, applications and SFC in real time, and deal with abnormal behaviors in time.

2) API security

The security center often provides data and services to the foreground system through API interfaces. The attacker can capture the interactive traffic of relevant APIs through sniffing tools, tamper with and call in large quantities to obtain sensitive data, or cause the security center to generate a large amount of garbage data, consume a large amount of resources, and even cause the security center to fail to work normally.

During the construction of the security center, encryption and signature technology shall be used to prevent data from being tampered with and replay attacks during the transmission process; API access mechanism shall be established to limit access frequency and authority. The interface call analyzes the malicious behavior and denies the service; Configure a dedicated API security gateway to control and manage the use of API interfaces.

4 Conclusion

The secure middle platform is the landing plan of the middle platform idea in the network security scenario, and also the architecture plan to solve the security dilemma in the digital transformation of enterprises. In the future, with the deepening of enterprise digital transformation, the intensification of capabilities and data is the only way By analyzing the security requirements of bank digital transformation, this paper studies and designs the security middle platform architecture for digital transformation, discusses the relevant technologies of security capability arrangement required by the middle platform construction, and proposes the example selection and routing optimization algorithm required by the security service function chain architecture.

Through the construction of the security center, the bank can integrate the security data collection capacity, break the security data island, improve the use of security data, and realize the unified management and sharing application of security data. Finally, it is supported by the security center. The rapid evolution of the upper layer business realizes the full scene coverage of the security protection business and improves the security operation efficiency.

References

1. Liuhongyan How enterprises protect cloud data security in cloud environment [J] Intelligence, 2016 (08): 232
2. Liliping Analysis of cloud security strategy for small and medium-sized enterprises [J] Logistics technology, 2016, 39 (10): 28–30
3. Zhang Ruyun Analysis of enterprise data security based on cloud environment [J] Office automation, 2018, 23 (03): 56–58+31
4. Yan Zhang Idea of enterprise employee information protection in cloud environment [J] Electronic testing, 2014 (11): 77–79
5. Huguohua, mengchengyun, Dai Zhibing, sunbin, liuzhenkai, yuhaibo, Li Bin, hewiqun, zhangzhiqi Research on cloud security system based on big data security [J] Information security research, 2020,6 (05): 404–420
6. Fenglei, cuipeng, liuboyu Research on dynamic cloud security management strategy of power enterprises in the context of cloud computing [J] Network security technology and application, 2015 (10): 37–38