Data Center Network Architecture Design for Cloud Computing

Yu Qing

Xinyang Vocational and Technical College, Xinyang , Henan, China

Abstract

In this paper, through the demand analysis of cloud computing data center network, the typical layer 2 Technology (virtual switch technology and tunnel technology) and cloud data center cross site layer 2 interconnection technology are analyzed and discussed in detail. This paper proposes MPLS VPN technology as an important technology of cloud computing data center network second tier expansion, and discusses VPLS network architecture and working principle in detail. This paper proposes the network architecture and implementation scheme of cloud data center based on MPLS VPN, and completes the network related tests. Finally, the characteristics of the system are summarized and analyzed. In this study, MPLS VPN technology is integrated into the existing cloud computing architecture to achieve the seamless integration of cloud computing resources and lay a theoretical foundation for the connection between virtual private cloud and public cloud. The experimental results show that according to the requirements of cloud computing data center, this research realizes the dual activity of network between data centers.

Keywords*: Cloud computing, data center, virtual switch, tunnel technology.*

I. Introduction

Data center is an integrated IT application environment formed by data centralization. It is the center of providing various IT application services and the center of data computing, network and storage. From the perspective of structure, data center is composed of different server sets and network infrastructure. Among them, the server completes the function of collecting data, and the network infrastructure is used to realize service use and data transmission [1-2]. Users can access server resources through the network. From the perspective of engineering technology, the establishment of the data center is to carry a specific network application, and the network application determines the distribution of servers, computing resources and storage resources in the data center, and then affects the network characteristics. Starting from the application, scale and user type of data center, data center can be divided into the following three categories [3].

(1) Internet Data Center (IDC) [4]: the main service providers of this kind of data center invest in the construction, and provide professional and standardized data storage and access services to customers by using carrier grade equipment, such as hosting, whole machine leasing, virtual host and other services. Users can build their own platform with the help of data center technology. Traditional Internet data center is transiting to cloud computing data center.

(2) Corporate data center (CDC) [5]: enterprise data center generally refers to the data center owned and used by the enterprise. It provides data processing and data access services for group users, internal organizations and partners. The operation and maintenance of data center equipment is in the charge of the internal T Department of the enterprise. In addition to traditional e.mail, storage and web services, enterprise dedicated data center also provides user specific services, such as enterprise development and testing platform, enterprise internal file system, online business applications, remote user registration services, etc.

(3) Campus Data Center [6]: efficiently serve teaching and scientific research through the establishment of data center infrastructure. The service objects are mainly students and teachers. There are various types of servers. The services provided mainly include e.mail, web services (as a management site to provide web access services for

ISSN: 0010-8189

students and teachers), OA system and multicast video services. This kind of data center equipment quantity is small, the network structure is relatively simple, generally uses two-tier structure.

As the innovation of computing mode and service management mode, cloud computing puts forward new requirements for data center network architecture [7-9]. The distributed and virtualized data center network is the basic condition of cloud computing. With the rapid development of cloud computing and data intensive computing technology, data center network (DCN) has become a research hotspot in the field of cloud computing. As the carrier of cloud computing infrastructure, data center network provides high reliability, high bandwidth and high availability data communication to distributed file system, storage resources and virtualization technology. With the advent of the era of data concentration, in order to reduce the operational risk and operational risk of data center, more and more enterprises pay attention to the disaster recovery in the same city and other places. The migration of virtual machine in cloud data center needs the interconnection of layer 2 network between data centers. VPLS, which combines the advantages of Ethernet and IP / MPLS, has gradually become an important technology to realize the interconnection of layer 2 network between data centers. In this study, MPLS VPN technology is integrated into the existing cloud computing architecture to achieve the seamless integration of cloud computing resources and provide a new idea for the virtualization of cloud computing data center network.

II. Requirement analysis

A. Data center network topology

In order to solve the problems of network stability, scalability and upper bandwidth bottleneck, new data center network architecture has been proposed by researchers to provide better optimized structure and communication services. The research of data center network topology refers to the specific needs of data center network, including network topology, server node addressing and interconnection rules setting. According to the current research and development situation, the network structure suitable for data center network can be divided into three types: switch centered network, server centered network and irregular network [10]. The network bandwidth and fault tolerance provided by the deployment of network structure directly affect the performance of data center network.

(1) Fat tree network structure

Fat - tree network structure which is shown in Figure 1 is a typical switch centric network. Fat - tree structure is a network structure constructed by cheap switches. This structure uses a large number of cheap switches and complex connections to replace expensive high-level switches, and realizes the equipment interconnection of large-scale data center network. These cheap switches have the same switching capacity and number of ports. They do not use uplink ports, but use downlink ports completely.

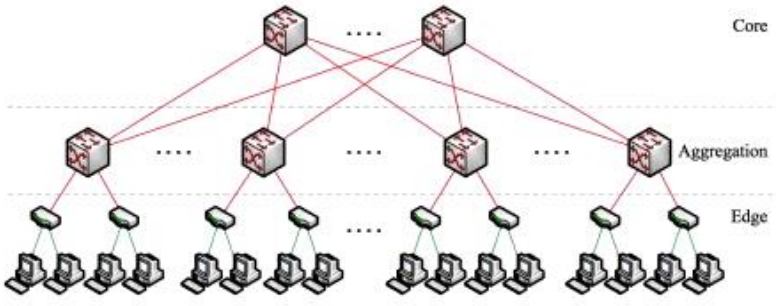

Fig 1: Fat - tree network structure

ISSN: 0010-8189

(2) Dcell network structure

Dcell network structure which is shown in Figure 2 is a kind of network type which is put forward by Microsoft Asia Research Institute. It is server centered and recursively defined. The hierarchical full connection method is used to generate the interconnection structure between small switches. The layered and highly symmetric three-dimensional mesh structure reduces the data delay and improves the fault tolerance and network bandwidth. Dcell0 is the smallest structure unit, which is composed of a special switch and several computers specially designed. As a node, this unit acts as the basic unit of the next layer structure, which ensures that the connection of each layer is a complete graph. It is based on the idea of recursion, using multi port network server and small switch to build the network topology. It can support routing fault tolerance and provide better aggregate bandwidth than tree structure and structure.

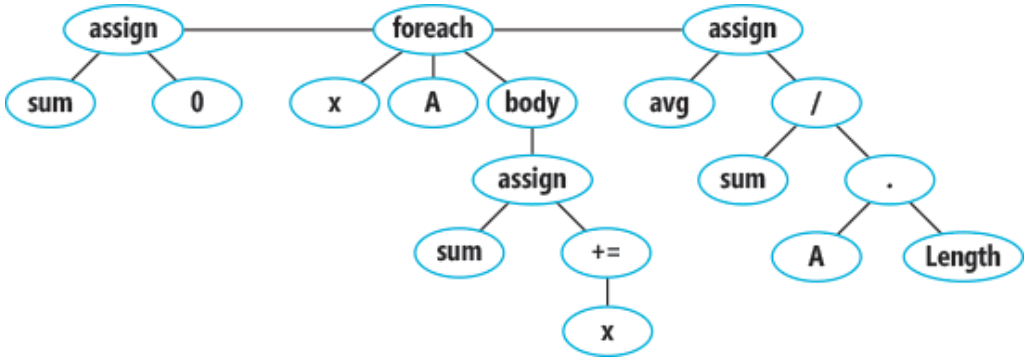

Fig 2: Dcell network structure

B. Development background and purpose

At present, many enterprises and companies operate in a distributed mode. Their headquarters are located in one city, which is the administrative center of the whole company. Many branches are set up in other cities according to the business distribution [8]. The branch company will report its own market situation and operation situation to the headquarters in a timely manner. The headquarters will summarize and analyze the situation reported by each branch company, formulate the operation strategy in line with the market law, and distribute it to the branches all over the country [9-10]. However, in order to ensure the security of data transmission, we have to adopt such technical means to process data.

The so-called security is a relative definition, there is no security policy or security. The protocol can guarantee absolute security. If there is no specific software or hardware reinforcement for the whole system components, it will only cause a waste of funds or resources. So in this paper, when designing the security scheme of the enterprise data security transmission system, we first need to understand and analyze its workflow and the information that needs to be interacted, determine which security standards to achieve, and then design and implement its security pertinently.

After the security goal is determined, the appropriate security policy or security protocol is selected according to the actual situation. The higher the requirement of security policy, the higher the complexity of the implementation process, and the implementation efficiency is inversely proportional to the complexity of the implementation process. Therefore, it is best to choose the most suitable security policy or security protocol for the design of the transmission process, so that the security line and the implementation efficiency can be well combined.

In view of this situation, we need to establish a safe and reliable data transmission system to provide a safe and reliable operation platform for the data interaction between the branch company and the head office. Through the use of the platform to achieve the unified management of users accessing the system, to ensure that from the

access to the company's internal resources, to data interaction, can realize the authentication of the user's identity and the authentication of data interaction authority, and encrypt the interactive data of both sides, so as to achieve the security of the whole process of data interaction.

III. Design and Implementation of Enterprise Data Security Transmission System

This system adopts B/S structure mode, uses Web browser as client, and concentrates the core part of system functions on the server. The advantage of adopting B/S structure is that it is easy to maintain and upgrade, all operations only need to be carried out for servers, and there is a richer and more vivid way to communicate with users. The browser accesses the server through Web Serve, and can interact with the server after obtaining authorization permission.

A. General design

Compared with the above requirements analysis, the overall architecture of enterprise data security transmission system is designed. The homepage on the server side of the head office is designed and implemented by JSP, and the update of homepage information is maintained by the network managers of the head office. The main work is to design the authentication module and the data interaction module. The overall structure is shown in Figure 3.

The function modules of the system are described as follows:

(1) Authentication module

When the branch users want to access the internal resources of the company, they first need to input the user name and password to verify the identity of the login. The server side compares the information entered by the user with the information stored in the database, and the information is checked correctly, allowing them to log in, and using the corresponding services provided in the system. If the information check fails, they refuse to log in.

(2) Data interaction module

When the authorized users of the branch log in to the module, they are allowed to upload or download data.

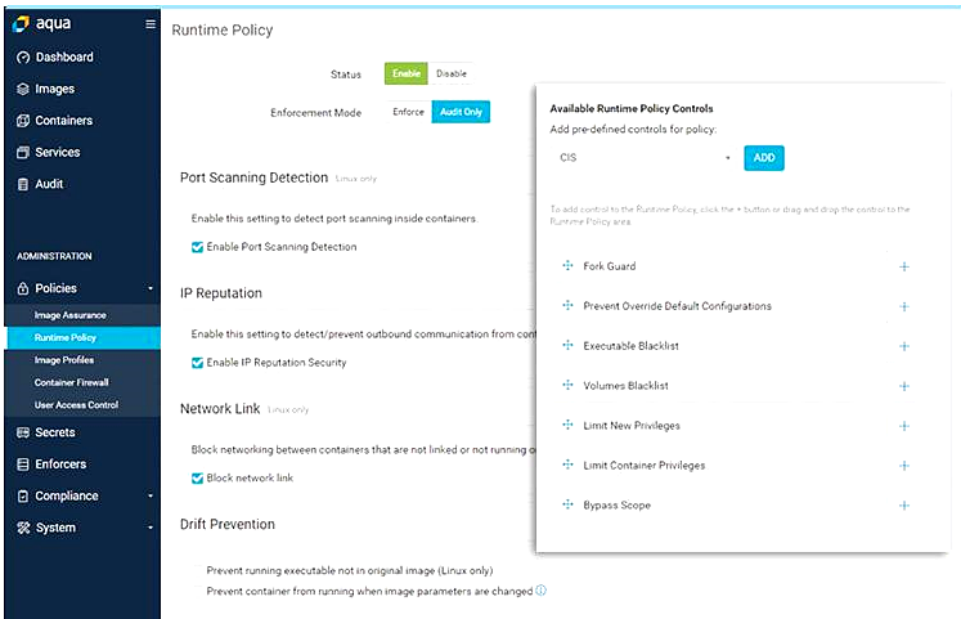

Fig 3: Overall structure diagram of enterprise data security transmission system

This system uses Java language in eclipse development environment and adopts B / S structure mode. Using web browser as client can improve the expansibility and maintainability of the system. It is at the bottom of the whole system. The core part of the system function is centralized on the server. The middle layer includes network and application server, which can interact data between client and database server. The top layer of the system is the database server, which provides transparent access to the lower layer to realize data storage and management. In the security policy and communication protocol, Kerberos + SSL is used to authenticate and authorize the user, and then encrypt the data interaction. The design of the system is shown in Figure 4.

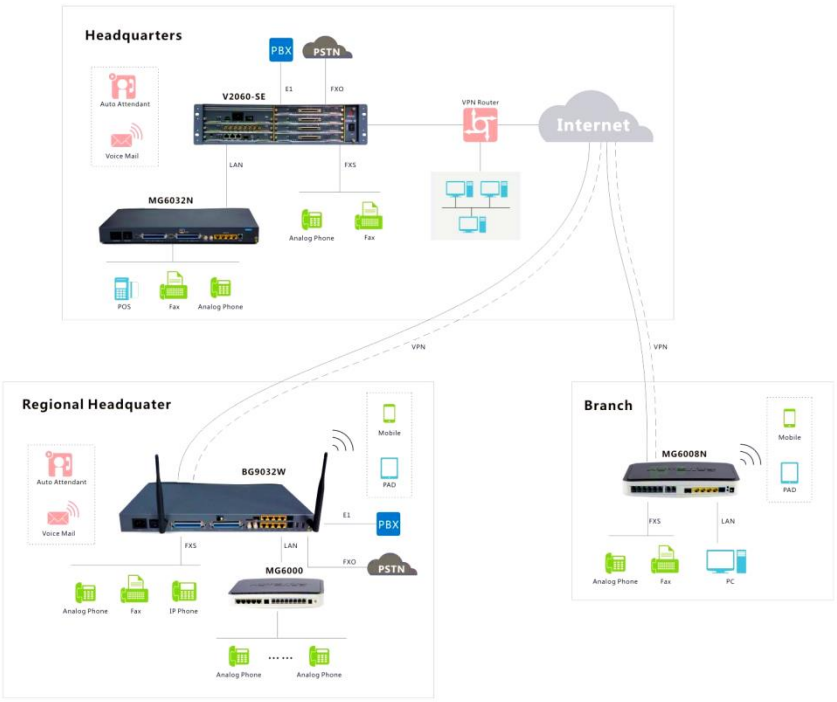

Fig 4: Architecture of enterprise data security transmission system

B. Design and implementation of system security policy

Through the analysis of the characteristics of some current communication protocols and the different application environment, the system selects the protocol as the communication protocol used by both sides of the communication. Through the analysis of the research on SSL protocol by domestic and foreign security experts and technicians, the results show that the authentication mechanism of SSL protocol has some security risks. Through the analysis of SSL handshake protocol authentication mechanism, this paper uses Kerberos identity authentication to improve SSL handshake protocol, and uses Kerberos + SSL security policy as the system security policy.

In SSL protocol, the handshake protocol is used to realize the identity authentication of both sides of communication. When RSA public key encryption is used, the unknown communication parties authenticate each other through the certificate mechanism. There are the following security risks:

SSL protocol supports extensible add in service model, which allows new authentication scheme and encryption method to be added to SSL protocol. Therefore, it is feasible to add Kerberos authentication method to SSL protocol. This paper discusses how to add Kerberos authentication scheme to SSL protocol. By defining the password group containing Kerberos authentication, as long as both sides support the encryption suite containing Kerberos authentication, the server can send the client the specific details of Kerberos authentication supported by itself, so that the communication parties can choose the Kerberos authentication method when carrying out secret negotiation.

In SSL handshake protocol, the server can choose to accept the certificate request from the client. If the server accepts the certificate request, it needs to return a corresponding type of certificate request packet to the client. The content of the packet mainly includes the certificate type list and the certification authority list. The specific content structure is shown in Figure 5.

Fig 5: Structure diagram of certificate request packet

When Kerberos authentication is used, the certificate type list should contain the Kerberos certificate type. The new certificate type list structure is shown in Figure 6.

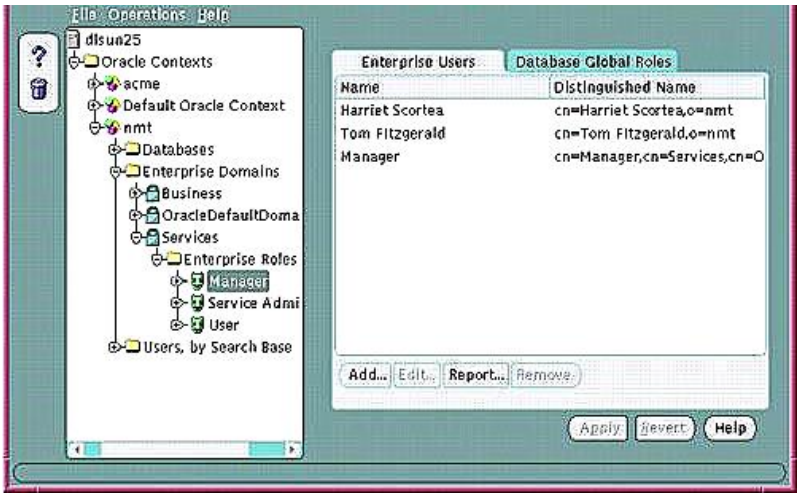

Fig 6: Certificate list structure

IV. Conclusion

With the progress of the times and the development of science and technology, the network will become closer and closer between people. In this case, distributed working mode has been widely used, how to ensure the reliability of communication and the security of information transmission is a problem that can not be ignored. This paper analyzes and summarizes the common security policies, security communication models and protocols, such as Kerberos authentication and SSL protocol. Although the functions of these security policies and communication models are very powerful, they also have their own security risks. How can we effectively use the advantages of these security policies and communication models, remove some functions that are not up to standard, and use some of these strategies and models to develop a security solution suitable for the actual application. Based on the above analysis, this paper puts forward the communication mode of Kerberos + SSL, and verifies the feasibility of the scheme by applying it to the enterprise data transmission system.

References

[1] Wei Yonglian, Yi Feng, Feng Dengguo, Yong W, Yifeng L. Network Security Situation Assessment Model Based on Information Fusion. Computer Research and Development, 2009, 46 (3): 353-362

[2] Xu Guoguang, Li Tao, Wang Yifeng. A Network Security Real-time Risk Detection Method Based

on Artificial Immune. Computer Engineering, 2005,31 (12): 945-949

[3] Jiang Wei, Fang Binxing, Tian Zhihong. Network Security Evaluation and Optimal Active Defense Based on Attack Defense Game Model. Acta Computer Sinica, 2009, 32 (004): 817-827

[4] Miao Yongqing. Stochastic Model Method and Evaluation Technology of Network Security. China Science and Technology Investment, 2017, 4: 314

[5] Bao Xiuguo, Hu Mingzeng, Zhang Hongli. Two Quantitative Analysis Methods for Survivability of Network Security Management Systems. Acta Communication Sinica, 2004, 25 (9): 34-41

[6] Li Weiming, Lei Jie, Dong Jing. an Optimized Real-time Network Security Risk Quantification Method. Acta Computa Sinica, 2009 (04): 793-804

[7] Yi Hua Zhou, Wei Min Shi, Wei Ma. Research on Computer Network Security Teaching Mode for Postgraduates Under the Background of New Engineering. Innovation and Practice of Teaching Methods, 2020, 3 (14): 169

[8] Yang Yi, Bian Yuan, Zhang Tianqiao. Network Security Situation Awareness Based on Machine Learning. Computer Science and Application, 2020, 10 (12): 8

[9] Li Zhiyong. Hierarchical Network Security Threat Situation Quantitative Assessment Method. Communication World, 2016, 23: 70-70

[10] Hu Wenji, Xu Mingwei. Analysis of Secure Routing Protocols for Wireless Sensor Networks. Journal of Beijing University of Posts and Telecommunications, 2006, 29 (s1): 107-111

ISSN: 0010-8189