Research and Application of Network Trusted Interconnection Technology

Wenjia Xie*, Zhe Wang¹, Ping Tang², Zhongmin Zhang¹ and Longsheng Chen³

¹ College of Information and Communication, National University of Defense Technology, Xi’an, Shaanxi, 710106, China
² Cloud network Operation Center, China United Telecommunications Corporation, Xi’an, Shaanxi, 710075, China
³ School of Automation and Information, Xi’an University of Technology, Xi’an, Shaanxi, 710048, China

*Corresponding author’s e-mail: xiewenjia17@nudt.edu.cn 84375886@qq.com

Abstract. In order to solve the problem of reliable information transmission between data centers and data sources, between data sources and between data centers, as well as the “network island” communication problem, a dynamic MPLS VPN method is proposed, the principle and steps of the method are introduced, and how to apply the method to the supporting platform is explained in detail.

1. Introduction

For security purposes, different networks have different security levels. Networks with different security levels cannot be connected, resulting in network islands. Data transmission is required between network islands due to service requirements. Data collection in the big data system requires real-time collection of data on the islands. The islands also need to be interconnected to achieve data sharing. Therefore, solving the problem of “network silo” and realizing the safe and reliable transmission of data is one of the important problems that need to be solved in supporting platform construction. During the interconnection of network islands, each of them must be independent, and the necessary data exchange can be carried out. During the data exchange, unrelated routes cannot be enabled.

Using VPN mutual access technology can achieve the above objectives. VPN technology has the feature of logical isolation. The main VPN communication technologies are as follows: IPSec VPN communication technology. However, IPSecVPN access technology is only applicable to IPSecVPN access, which is difficult to meet the construction of multiple network environments for supporting platforms and data sources. Dynamic MPLS VPN enables VPN access and applies to multiple networks.

2. Dynamic MPLS VPN

2.1 Method Principle

Dynamic MPLS VPN (DMVPN for short) uses MPLS VPN technology to establish connections to achieve trusted network interconnection and secure data transmission. VPN nodes that need to access
each other register their identities with the management server. Only nodes with registered IDENTIFY information can communicate with each other through the VPN. When a VPN node requests to communicate with another VPN node, the VPN node sends a connection request to the management server. After receiving the connection application, the management server queries the access rule set to determine whether the application can pass. If the connection request fails, the connection will not be established. If the connection request succeeds, the connection will be established between nodes that access each other. When the connection between nodes is allowed, the management server allocates new labels and establishes a label switching path (LSP) between VPNS using MPLS. The management server sets filtering rules based on node information and access rules, and delivers the filtering rules to the USER edge router CE of the VPN where the node resides. The data transmission of VPN nodes strictly follows filtering rules and implements strict content detection mechanism. After the CE filters the packets, the PACKETS arrive at the PE router (LER). The PE adds new labels to the packets and transmits them through LSP. When the specified transmission period reaches or data transfer ends within the specified transmission period, the rules for mutual access between nodes are deleted, and nodes cannot communicate with each other. If no VPN is connected to each other, the label information and LSP are deleted.

2.2 Implementation of dynamic MPLS VPN

2.2.1 Registering node Identities

Nodes that join the mutual access system must register their identity information with the management server. [1] The process of identity registration is actually the process of the management server reviewing the interconnection requirements and establishing the mutual access rule set. Each node submits its registration information to the management server through the user edge router CE of the VPN. The registration information includes the VPN where the node is located, IP address and MAC address, VPN where the destination node is located, IP address and MAC address of the destination node, data flow direction (incoming or outgoing), port number, and expected transmission duration. After receiving the registration information, the management server determines whether the registration is successful based on the actual situation and fills the passed registration information in the corresponding position of the mutual access rule set.

2.2.2 Establishing a connection

Establishing a connection between two nodes using DMVPN includes three stages: application stage, establishment stage and transmission stage. Application stage. When node I in VPN1 has service requirements and needs to transmit data with node J in VPN2, node I sends a Connectes Request message to the management server through CE1, the edge router of VPN1, to apply for establishing a connection with node J. The Connect_Request message contains the IP and MAC addresses of node I, the ID of VPN1, the IP and MAC addresses of node J, and the id of VPN2. Establishment stage.[2] The management server parses the Connect_Request message to obtain the IDENTIfiers of VPN1 and VPN2, searches for the level-1 communication rule table in the communication rule set, and checks whether the corresponding label information is empty by comparison. If it is empty, CE1 and CE2 are not connected. If it is not empty, CE1 and CE2 are connected. Transmission stage. After the LSP is established, node I and node J are connected through CE1 and CE2. In this case, data can be transferred between nodes. Data is transferred strictly according to filtering rules. In addition, the CE checks the transmitted content according to the requirements of the management server. Data that does not meet the requirements is filtered out.

2.2.3 Connection Deletion

The connection between nodes will be deleted when the data transfer between nodes ends within the transmission period or when the specified transmission period is reached. According to the reason for connection deletion, connection deletion between nodes can be divided into two types:
terminate-request and out-time.

3. Limitations of DMVPN method

Using DMVPN method for network interconnection, can achieve fine-grained control by time, by node, by direction, by content; There is no requirement on the VPN type of the two parties. After the information exchange is complete, the links are completely deleted and the routes do not stay on for a long time. However, this approach also has the following limitations:

(1) High performance requirements for the management server. [3] The management server is not only responsible for DMVPN method request application, but also responsible for identity registration and link disconnection after information exchange. These have high demands on the performance of the management server, especially I/O performance. The high demand for VPN access causes the performance bottleneck of the management server. If the demand for simultaneous VPN access exceeds the threshold of the management server, the communication services will be seriously affected.

(2) This method cannot be used to establish channels for trusted interconnection and information transmission between VPNS managed by different management servers. Multiple VPNS are allocated based on services. Different VPNS may belong to different management servers. The DMVPN method requires that VPNS with communication requirements belong to the unified management server to facilitate identity registration and connection notification. When VPNS belonging to different management servers need to exchange data due to service requirements, the DMVPN method cannot be applied due to different VPN affiliation. In view of the above problems, the hierarchical communication method can effectively reduce the pressure of the server, expand the application scope of DMVPN method, and establish a secure and reliable communication link between VPNS belonging to different management servers, so as to achieve the purpose of information exchange.

4. Application of DMVPN and hierarchy interworking method in support platform

There are two types of management servers: Primary DATA center management server and secondary data center management server. The level-1 DC management server is the root management server, and the level-2 DC management server is the leaf management server. The support platform divides connected application systems AS into VPNS, and each VPN is called ASmt. M indicates the number of the secondary data center, and T indicates the number of the application system. The working steps of the hierarchical interworking method in the supporting platform are as follows:

4.1 Communication with THE VPN of the Level-2 DC Management Server (AS11 and AS12 are Used as Examples)

4.1.1 Connection Request

The management server in secondary data center 1 receives a connection request from node I in AS11 under its administration to communicate with node J under AS12. The management server in level-2 DATA center 1 searches the global status table first and finds information about AS12, indicating that
AS12 is managed by the management server in level-2 data center 1. [4]The administration server then looks up the set of rules for mutual access based on the request information. If no matching entry is found, the request is rejected and a request failure message is sent to node I to stop connection establishment. If a matching entry is found, the management server sends the application success message to node I and the set data transmission time between the two parties. [5]The management server also sends a connection establishment notification message to node J, notifying it that node I is applying to establish a connection with it, and sends the basic information of node I (mainly THE IP and MAC address of I, and the identity of AS11) and transmission time to node J.

4.1.2 Connection Establishment
After the connection request passes, the level-1 access rule table of the management server is searched based on the identification of AS11 and AS12. If no label information is displayed, it indicates that the connection between AS11 and AS12 is not established. The management server randomly generates the label information and adds it to the level-1 access rule table. If the label information is not empty, it indicates that AS11 and AS12 are connected, and the nodes use the label information for data transmission. The management server delivers the label information, and AS11 and AS12 establish a label switching path based on the label information, that is, a data transmission channel between nodes I and J. The management server sends the filtering rules generated in the level-2 access rule table to the edge routers of AS 11 and AS12. Data is transmitted between nodes I and J based on the filtering rules.

4.1.3 Connection Deletion
When the specified communication period arrives or information transmission ends within the specified communication period, the LSP between AS11 and AS12 is deleted using the out-of-time or terminate-request deletion method.

4.2 VPN Communication between Management Servers in Different Level-2 DCS (AS11 and AS21 Are Used as Examples)
AS11 and AS21 are managed by the management server in secondary data center 1 and 2 respectively. The steps for AS11 and AS21 to communicate with each other include connection request, connection establishment, and link deletion.

4.2.1 Connection Request
Node I in AS11 submits a connection request to the management server in level-2 data center 1, requesting to communicate with node M in LEVEL-2 data center 1. The management server in Level-2 data center 1 searches the global status table and fails to find information about AS21, indicating that AS21 is not under the jurisdiction of level-2 data center 1. Level-2 DC 1 The management server submits connection requests to the level-2 DC management server. After receiving the connection request, the level-1 DC management server extracts information about AS21 and checks the status table. If no information about AS21 is found, AS21 does not exist in the support platform, and the level-1 DC returns a connection failure signal. The signal is returned to node I from the management server in secondary data center 1. If information about AS21 is detected (for example, AS21 is managed by the management server in level-2 data center 2), level-1 data center determines whether data needs to be transferred between AS11 and AS21 based on the remarks of AS11 and AS21 in the global status table and the actual situation. If no, the system rejects the connection and returns a connection failure message. If yes, the level-1 DC management server queries AS21 about the existence of node M through the management server in level-2 DC 2. If node M does not exist, the level-1 DC rejects the connection request from node I and sends a connection failure message to node I. If node M exists, the connection request is approved. The level-1 DC management server sends the connection request to AS21 through the management server in level-2 DC 2, including the information about AS 11 and the address of node I.
4.2.2 Connection establishment
After the connection request passes, the level-1 DC checks whether AS11 and AS21 are connected. If yes, use the existing label. If no, the level-1 DC management server randomly generates new label information, sets a rule filtering set based on connection requests and actual requirements, and then sets filtering rules for AS11 and AS21 communication based on the rule set. The level-1 DC management server delivers the label information and filtering rules to the management servers in level-2 DC 1 and Level-2 DC 2. The management servers then send the label information and filtering rules to the PE and CE devices of AS11 and AS21 respectively. At the same time, the level-1 DC management server sets the communication duration for VPN1 and VPN3 based on the history and actual situation, and sends the notification to AS11 and AS21. AS11 and AS21 establish LSPs based on the new labels to exchange data and filter information according to the filtering rules.

4.2.3 Connection Deletion
The LSP between AS11 and AS21 is deleted when the specified communication period arrives or information transmission ends within the specified communication period. The initiator of LSP deletion varies according to the deletion reason. When information is exchanged between AS11 and AS21 within the specified communication period, the CE devices of AS11 and AS21 send a message to the management server (secondary DC management server). After receiving the message, the management server sends the message to the primary DC management server. After receiving information transmission signals from AS11 and AS21, the level-1 DC management server sends a filtering rule deletion signal to the level-2 DC management server. The signal is finally sent to the CE devices of AS11 and AS21. The CE deletes filtering rules after receiving the filtering rule deletion signal. If no connection is required between AS11 and AS21, the level-1 DC management server deletes the label information to completely delete the LSP between AS11 and AS21. When the communication time comes and the parties have not completed the information exchange, or the level-1 data center management server does not receive or only receives a signal from AS11 and AS21 to complete the information transmission within the specified time, The level-1 DC management server sends a connection timeout signal to the CE devices of AS11 and AS21 through the management server of level-2 DC 1 and level-2 DC 2 respectively, and sends the information about deleting filtering rules. The CE devices of AS11 and AS21 delete the filtering rules of nodes I and M from the filtering rules table after receiving the connection timeout and filtering rules deletion signals. When no information is transmitted between AS11 and AS21, the level-1 DC management server deletes the label information to delete the LSP between AS11 and AS21. The hierarchical interworking method makes it possible for VPN communication between different management domains, expands the geographical application scope of DMVPN method, and facilitates data sharing between VPNS across regions and across data centers, which is suitable for distributed deployment of data centers on supporting platforms.

5. Conclusion
This chapter in view of the support platform of different communication under the network environment, put forward the solution to "network island" unicom, implement the data exchange between the dynamics of the MPLS VPN method, based on the characteristics of the support platform has a wide range of each hierarchy method is proposed, the method of dynamic MPLS VPN can across a wide range of areas, means a management conditions.

References
[1] (2021)TCPIP and VPN Li Zongb. Peking University Press.
[2] Wang D. (2021) Huawei Router Learning Guide 2nd Edition Self-study Guide for Huawei Routers Huawei Traditional VPN Technology Principles Huawei VPN Deployment Cases Huawei AR G3 series router configuration guide. Posts and Telecommunications Press, Beijing.
[3] Yang Dx. (2021) Information security network Space SECURITY VPN Technology. Tsinghua University Press, Beijing.

[4] John Donovan. (2021) Software-defined journey to the Network Building a smarter, faster and more flexible future network SDN Technical Books NFV Network Function Virtualization VPN 5G network Cloud Edge computing. Posts and Telecommunications Press, Beijing.

[5] Yang Dx. (2021) Information security network Space SECURITY VPN Technology. Tsinghua University Press, Beijing.

[6] LiuDN. (2021) MPLS and VPN Architecture. Posts and Telecommunications Press, Beijing.