IPSec-VPN Availability Research and Simulation

Fan Yang [1, a] , Lizhen Zhao [2,b]

[1] School of Computer Science, Zhaoqing University, Zhaoqing, Guangdong, China

[2] Educational Technology and Computer Center Zhaoqing University, Zhaoqing, Guangdong, China

[a]Yangfan9@zqu.edu.cn, [b]sdzlz@zqu.edu.cn

Keywords: Availability; IPSec-VPN ; GNS3 ; Simulation ; Redundancy

Abstract. For the technical defects of IPSec-VPN on the aspect of reliability, we analyze unreliable factors of site-to-site IPSec-VPN topology model, propose to use link redundancy, equipment redundancy, routing redundancy and other technologies, construct high available IPSec-VPN ideas and methods, and conduct simulation through the virtual network tool GNS3 to test whether the opposite gateway of IPSec-VPN can work normally in case of the current link and the current route or in case that the current equipment has failures so as to verify its availability. The simulation results have shown the correctness and the actual availability of the method.

Introduction

By comprehensively applying tunnel technology, key management and exchange technology[1,2], authentication technology and encryption technology[3,4], etc., IPSec-VPN has established a logically secure information transmission channel on the insecure public network so that dispersed and independent users on the physical location can transmit information mutually via this secure logical channel so as to provide a secure communication environment with the abilities of anti-eavesdropping, forgery and tamper resistance[5]. However, in terms of reliability, IPSec-VPN only has provided DPD technology[6] used for monitoring whether the opposite IPSec-VPN gateway is available, which has solved the problem that when the opposite IPSec-VPN gateway is not working properly, we can stop the local IPSec-VPN gateway and use the original security association for encryption and send data so as to avoid the waste of a lot of packet loss and routing resources. However, DPD technology can't solve the problem of rapid restoration of security association after IPSec-VPN gateway fails.

Based on analyzing the reliability factors that affect the site-to-site IPSec-VPN topology model, this paper has proposed to use link redundancy, equipment redundancy, routing redundancy and other technologies, construct high available IPSec-VPN ideas and methods, and conduct simulation through the virtual network tool GNS3[7] to test whether the opposite gateway of IPSec-VPN can work normally in case of the current link and the current route or in case that the current equipment has failures so as to verify its availability. The simulation results have shown the correctness and the actual availability of the method.

Main factors affecting IPSec-VPN availability

IPSec-VPN mainly has two application modes: site-to-site mode and remote access mode, in which the site-to-site mode is the most representative. In this mode, different branches can deploy IPSec-VPN gateways from their own local network to Internet outlets, establish IPSec-VPN channels via Internet and achieve interconnection and secure communications between remote LANs. Both the site-to-site mode and the remote access mode need at least one IPSec-VPN gateway erected on the public network outlet from the relevant LAN to Internet so as to establish IPSec tunnels with other IPSec-VPN gateways or remote mobile users and provide services of secure communications. IPSec-VPN gateway is the only way for all IPSec communications, so it is the single fault point, once it goes wrong or is not working properly, it will affect the entire VPN applications[8]. The factors that affect IPsec-VPN system s normal applications are mainly:

（1）Equipment failure——fundamentally, IPSec-VPN gateway is a complex computer system composed of hardware and software running on the basis of the hardware, both the hardware and the software are likely to fail, and the traditional IPSec-VPN gateways are stand-alone systems, so once the gateway doesn't work normally, the entire system will not provide normal IPSec communication services.

（2）Link failure——the basic idea of VPN is to use the existing public network to provide secure communication services, therefore, the network link used by VPN system is not included in the construction scope of VPN system and the service quality is not controlled by VPN system. The network link is affected by various natural or man-made factors, so it is also likely to fail and is unable to provide communications.

（3）Performance bottleneck——IPSec-VPN itself is a compute intensive system and needs to operate a large number of encryption and decryption computation of messages; with the expansion of the scale of application, there's a sharp increase in the number of messages to be processed, and because of the characteristics of applications, the situations of sudden high capacity in a short period of time are common, which have made the performance of VPN gateway become the bottleneck to restrict the applications.

Construction of a high available IPSec-VPN topology model

IPSec-VPN availability analysis

The availability of IPSec-VPN is related to its reliability and maintainability; for users, the availability reflects the percentage between the time that IPSec-VPN system provides services normally and the total time that the system is running, that is, if the availability of IPSec-VPN is high, the percentage of the time of providing normal services for users will be high. This shows that on the one hand, IPSec-VPN system can normally operate without failures for a long time, on the other hand, once IPSec-VPN system fails, the time required for repairing the system is very short[9]. In order to provide a high available IPSec-VPN system, we can adopt equipment redundancy, link redundancy, routing redundancy and other technologies.

Construction of a high available IPSec-VPN network topology

Figure 1 is a high available IPSec-VPN network topology constructed based on redundancy technology to provide the system's backup and recovery capabilities through adding redundant links and redundant equipment. Router VPN-Gate1 simulates IPSec-VPN gateway of branch network in application scenarios, router VPN-GateA simulates IPSec-VPN main gateway of headquarters

network in application scenarios, router VPN-GateB simulates IPSec-VPN backup gateway of headquarters network in application scenarios, router R2 simulates ISP network in the public network, router R5 and switch L2-SW are used to simulate headquarters network in VPN application scenarios, and Loopback0 interfaces added in both sites respectively simulate the subnet in headquarters network and branch network.

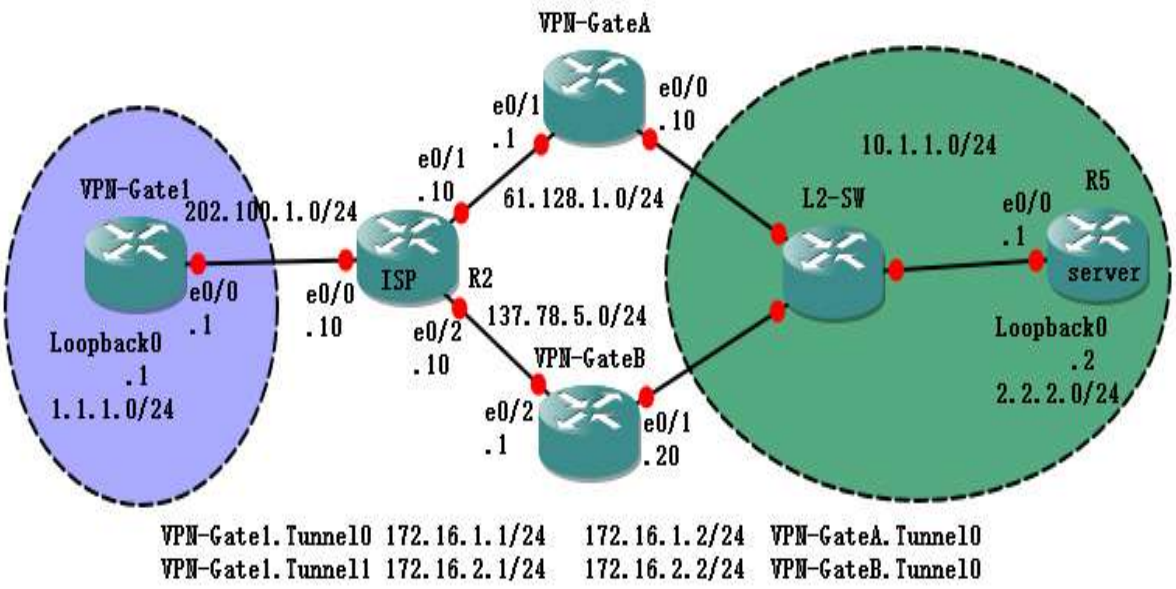

Figure 1 High available IPSec-VPN
simulative network topology

High available IPSec-VPN network control mechanism

Based on figure 1, there are a variety of availability control schemes, such as using STP Spanning Tree and HSRP Hot Standby Routing to achieve the reliability control of redundant links. In this research, Tunnel technology is used to respectively build two channels Tunnel0 and Tunnel1 between VPN-Gate1, VPN-GateA and VPN-GateB to achieve the logically direct connection between VPN-Gate1, VPN-GateA and VPN-GateB, which can configure the dynamic routing for the entire network based on EIGRP protocol and form a failure-finding and backup handoff mechanism driven by routers. Under normal circumstances, load balancing is achieved through routing protocols: when VPN gateways or the corresponding links fail, routing protocols will discover routing failures and replace routes for switching links without delay so as to ensure the availability of IPSec-VPN.

Configuration of IPSec-VPN high availability

This paper omits the relevant configuration of IPSec of three VPN gateways: VPN-Gate1, VPN-GateA and VPN-GateB and mainly introduces the configuration of availability strategies. The main configuration information is listed in table 1 below.

Table 1　Main configuration information of IPSec-VPN high availability

（1）Configure main Tunnel0 and backup Tunnel1on VPN-Gate.	（2）Configure main Tunnel on VPN-GateA.
int tunnel 0 ip address 172.16.1.1 255.255.255.0 tunnel source 202.100.1.1 tunnel destination 61.128.1.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec-profile int tunnel 1 ip address 172.16.2.1 255.255.255.0 tunnel source 202.100.1.1 tunnel destination 173.78.5.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec-profile ip route 0.0.0.0 0.0.0.0 202.100.1.10	int tunnel 0 ip address 172.16.1.2 255.255.255.0 tunnel source 61.128.1.1 tunnel destination 202.100.1.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec-profile ip route 0.0.0.0 0.0.0.0 61.128.1.10
（3）Configure backup Tunnel on VPN-GateB.	（4）Configure dynamic routing based on tunnel.
int tunnel 0 ip address 172.16.2.2 255.255.255.0 tunnel source 137.78.5.1 tunnel destination 202.100.1.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ipsec-profile ip route 0.0.0.0 0.0.0.0 137.78.5.10 After the above configuration is over, check the interface configuration of each gateway and the protocol of tunnel port has already been established.	In the network of figure 1, uniformly use EIGRP routing protocol, and the specific configuration of VPN-Gate1 is as follows: router eigrp 1 network 1.1.1.0 0.0.0.255 network 172.16.1.0 0.0.0.255 network 172.16.2.0 0.0.0.255 no auto-summary The routing configurations of VPN-GateA, VPN-GateB and R5 are similar, so we will not repeat them.

Simulation operation and analysis

Operate the network in figure1, when both the main Tunnel and the backup Tunnel are working properly, encrypted data streams pass both the Tunnels, which plays the role of load balancing: when one Tunnel or gateway fails, the other Tunnel and gateway works normally to provide a secure encrypted channel, as shown in figure 2, which has significantly improved the availability of IPSec-VPN. When all the two Tunnels or the two gateways fail, the secure encrypted channel will not be provided.

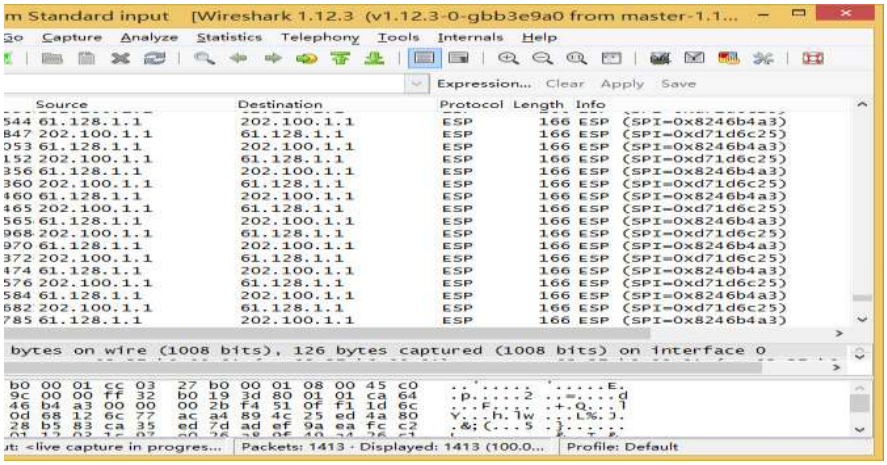

Figure 2 Normal IPSec-VPN with one failed link or gateway

Conclusions

Based on redundant links and redundant VPN gateways, this paper has built a high available site-to-site IPSec-VPN network topology, and on this basis, taking VPN demands of enterprises as the model, we respectively established the logical tunnels from the branch VPN gateway VPN-Gate1 to the headquarters VPN gateway VPN-GateA and VPN-GateB and achieved the availability control of IPSec-VPN through EIGRP routing protocol. This method has practical application value in the real network engineering and the teaching of network engineering specialty.

Reference

[1]The network working group, D.Piper. The Internet IP Security Domain of Interpretation for ISAKMP[J].RFC2407,1998:236-264.

[2]The network working group, D.Harkins, D. Carrel. The Internet Key Exchange (IKE). RFC2409, 1998:79-92

[3]The network working group, S.Kent,R. Atkinson.IP Authentication Header[J]. RFC2402, 1998:144-169.

[4]The network working group, S.Kent, R.Atkinson. IP Encapsulating Security Payload (ESP) [J]. RFC2406, 1998:34-48.

[5]Qin Ke. Cisco IPSec VPN Practical Guide [M]. Beijing： People’s Posts and Telecommunications Press，2012：1-54

[6]Qin Ke. Cisco IPSec VPN Practical Guide [M]. Beijing： People’s Posts and Telecommunications Press，2012：111-113

[7]Introduction to GNS3 [EB/OL]. http://www.gns3.net/gns3-introduction/,2012-11-20

[8]Zhang Yuhe. Research of High Available IPSec Virtual Private Network[D]，[PhD Thesis of Huazhong University of Science and Technology]，Hubei：Huazhong University of Science and Technology，2009,11

[9]Yi Jianxun, Jiang Lalin, Shi Changqiong. Computer Network Design[M].Beijing：People's Posts and Telecommunications Press，2011：116-130