Implementation of GRE Over IPsec VPN Enterprise Network Based on Cisco Packet Tracer

Chong Wang
Hainan College of Software Technology, Qionghai 571400, China
26782081@qq.com

Jing-you Chen
Hainan College of Software Technology, Qionghai 571400, China
1269042033@qq.com

***Abstract*—Along with the increasing prominence of network security problem, VPN (Virtual Private Network, VPN) technology provides a solution of economic remote access for the enterprise. As the IPSec protocol is able to provide the highest level of security, using IPSec VPN to build security Intranet has become a trend. Since the IPSec (Internet Protocol Security) does not support the encryption of multicast and broadcast packet, GRE (Generic Routing Encapsulation) tunnel is needed to encapsulate multicast and broadcast packets to unicast packet. By encrypting the GRE with IPSec, the data security is guaranteed and the problem of VPN scalability is solved.**

Keywords-VPN; GRE; Intranet; IPSec; IKE

I. INTRODUCTION

Enterprise informatization is the only way for the development of all enterprises, especially large enterprises. These enterprises are characterized in large scale, with more than one division or branch. Information exchange is needed among them, some of which involves the enterprise's business secrets. If the enterprise information is transmitted through the Internet, there will be many problems in safety. The Internet has the advantage of cheapness, but it is not safe, while, by contrast, leased line is safe, but more expensive. Then, how to ensure the confidentiality and integrity of information exchange between the headquarters and the divisions of the enterprises? How to make the cost of connection not as high as that of leased line? In order to solve this problem, the VPN (Virtual Private Network) was born. It is not only secure, but also low-cost. VPN technology provides a solution of safe and cheap remote access for enterprises. The secure enterprise virtual private network was established in the Internet by using IPSec security tunnel. Thereby the communication could effectively guarantee the security of enterprises.

II. GRE OVER IPSEC VPN

A. Brief Introduction of VPN

VPN (Virtual Private Network) is a kind of technology that uses public network to build the special private network, and it is the "line in the line". Data is spread through a secure "encrypted tunnel" in the public network. Building a special communication line between two or more enterprises Intranet located in different parts to connect the Internet, is just like establishing a special line. But it doesn't need to build a real physical line like optical cable. Enterprises only have to hire local special data line and connect it to the local Internet, so that the institutions can transmit information to each other.

Through the integrated use of Internet technology, access of interview technology, encryption technology, and certain user management mechanism, the user can make use of the existing public Internet to safely, securely, and undisturbedly interview the remote internal network resources. Compared with the traditional private network, VPN technology greatly reduces the cost. It is convenient, safe, standard, and becomes the main technology in achieving enterprises' cross-regional secure network interconnection. VPN can be divided into three categories: (1)Internal virtual network (Intranet VPN): the safe connection between the headquarters and branches; (2) Remote Access to virtual network (Remote Access VPN): employees' remote access to the company network server. Generally, it should have encryption, identity authentication, filtering, and other functions; (3) Enterprises expanding virtual network (Extranet VPN): providing security for the enterprise's business partners, suppliers and customers, mainly ensuring the data not being modified in the process of transmission and protecting the network resources from external damage.

VPN mainly adopts two technologies: tunnel and security technology. Current tunnel technology is mainly supported by three kinds of protocol: PPTP, L2TP and IPsec. The main mission of tunnel technology is completing the secondary encapsulation of IP packets in order to realize the transmission of enterprise's private address on the public Internet. To ensure the security of transmission, a secure means of encryption shloud be used to ensure the privacy and integrity of the data. Security technology mainly includes MPPE, IPSec and other encryption algorithm. IPsec provides security services in IP aspects. On the tunnel and encryption technology, IPSec has already become a widely-used and open VPN security protocols, which ensures the interoperability running between the TCP/IP protocol and the VPN. IPsec defines a set of standard protocols to protect the privacy and integrity and supports a series of encryption algorithm like DES 、3 DES. It checks the integrity of the

transmission of data packets to ensure that the data has not been modified. It has the function of authenticating the source data.

B. IPSec

IPSec Internet Protocol Security is a set of protocols providing IP security in network layer defined by IETF (Internet Engineering Task Force). Being able to provide the certification of data integrity, the identification of data sources and the protection of preventing retransmission, IPSec is one security technology applying to all Internet communication at present. IPSec system including three main security protocols, namely the AH (Authentication Header), ESP (Encapsulation Security Payload) and IKE (Intemet Key Exchange).

The realization of the IPSEC VPN is mainly composed of two stages. The first stage is IKE1 (Internet key exchange), whose main task is carrying an authentication on both sides of communication, and building a secure data channel at both ends. The parameters, which used to establish IKE secure channel under negotiation, mainly have the encryption algorithm, hash algorithm, DH algorithm, identity authentication algorithm and survival time. A collection of these parameters in this stage is called strategy set, and the purpose of consultation is making the strategy set on both sides the same. The second stage is IKE2, whose main task is to negotiate secure parameters in this channel, mainly including the encryption algorithm, hash algorithm, encapsulation mode, survival time and security protocols, and eventually to negotiate the same SA (Security Association). IPSec protocol can be set in two modes: tunnel mode and transmission mode. Under the tunnel mode, IPSec encapsulates lPv4 packets to the secure IP frame. Tunnel mode is the safest one, but it will lead to a larger system overhead. Transmission mode is to protect the security of end-to-end, that is, it will not hide the routing information in this mode.

C. GRE

Encapsulating the datagram of some certain network layer protocol (such as IP, IPX, AppleTalk, etc.), GRE (Generic Routing Encapsulation) makes it possible for the encapsulated datagram to transmit in another network layer protocol (IP). The transmission channel of heterogeneous network is called tunnel. As a kind of encapsulation methods, its practicality is very strong, which makes GRE encapsulation generally used in the VPN. However, the GRE tunnel itself doesn't support data encryption. There should be other protocols like IPSec to realize the data transmission encryption. GRE can provide low overhead tunnel. The encapsulation format of GRE is defined in RFC1701 / RFC1702, that is, the method of how to use a network protocol to encapsulate another network layer protocol. GRE tunnel is defined by the source IP and destination IP at the both ends of tunnel, and it can support various routing protocols, such as RIP, OSPF, IGRP, etc.

D.The advantages of ipsec vpn

The advantages and applications of IPSec VPN in the enterprise network have shown increasingly. On the IP transmission, the IPSec VPN technology uses an encrypted tunnel to transmit the content of the internal private network on the public network, and at the same time, it guarantees the security of the internal data, so as to realize the interflow of data, voice and video between enterprise headquarters and branches. Nowadays, the VPN has been regarded as a main method to connect remote branches and mobile users by many enterprises to build the virtual service network. Large numbers of domestic enterprises begin to consider this method and even gradually come into effect. There are following advantages for enterprises using the Internet to build their own IPSec VPN.

1) *Economic:* No need to undertake the expensive rent cost for fixed lines. Long-distance charge for DDN, frame relay and SDH increases with the increasing communication distance, the farther the branches, the higher the rent cost. While the Internet access charge only needs the local cost, no matter how far is the branch, the charge is the same. Therefore, used as transmission backbone, the Internet is dog-cheap, and still has higher bandwidth. In addition, the VPN device is superiorly in its function and low cost.

2) *Flexible:* Internet can be connected by the l0M, 100M port, and 2M or lower speed port, as well as the cheap DSL, even the dial-up connection, which makes it the most famous numerous end connections. An IPSec VPN network can connect the branches at any location, even across oceans. IPSec VPN can connect to a small quantity of branches at bargain prices, as well as numerous branches. The core equipment of IPSec VPN has good extensibility, a port can be connected with thousands of branches at the same time, including divisions and mobile office users, rather than needing a port corresponding to remote users like SDH, DDN. Remote IP voice and video business can also be transmitted to remote branches and mobile users, providing convenient conditions for modern offices together with the data business, and saving a lot of telephone charges.

3) *Safe:* The significant characteristic of IPSec VPN is its security, which is the root of its internal data security. On the VPN switches, it ensures the security by supporting all the leading channel protocols, data encryption and filter/firewall, as well as realizing authorization by the RADIUS, LDAP, SecurID and many other ways. At the same time, the VPN devices provide a built-in firewall function to transmit the flow from public to private network interface outside the VPN channel. In addition, this technology can also pass the authentication like RADIUS, PAP, CHAP, Tokens, X.509, LDAP and SecurID, etc.

4) *Redundant Design:* VPN devices can provide redundant mechanism, guaranteeing the reliability of the link and equipment. VPN core equipment in the center node provides hardware redundant designs like redundant CPU, redundant power source. When the link fails to work well,

VPN switches support static tunnel for failure recovery function, and its secure IP service gateway can realize the load balancing between multiple routing paths and multiple switches. Besides, in the connection, the VPN client will automatically select the backbone node of this area which is set in the communication list, and automatically choose other VPN switches according to the list settings when the regional node fails, so as to achieve the purpose of the connection.

5) *Effective Management:* The split channel characteristic of VPN switches provides the supports of visiting the Internet, Extranet and local network for IPSec client at the same time. This technology can set permissions, allow users' access, such as local print and file sharing, direct Internet and secure outside network. This characteristic makes it possible for users to use the network resources rationally and conveniently under the safety condition, both secure and flexible. Routing protocols are needed by the multiple users and complex routings to make the entire web address management convenient and effective. With the help of RIP & OSPF, VPN devices' connection and extension are as routers, which is suitable for the continuous expansion of network. What's more, the dynamic routing protocol can be supported in the encrypted tunnel. Managers can manage the remote node through the management of software and remote configuration .

III. DESIGN PRINCIPLES

A. Key steps for configuration

IPSec configuration between routers uses IPSec connections, and it needs to configure a virtual tunnel as a secure link for secure and reliable communication between the two networks. Taking IPsec encryption algorithm using pre-shared key for example, the IPsec VPN configuration process is as follows:

1) Configure IKE strategy: including hash algorithm, encryption algorithm, and lifetime;

2) Configure pre-shared key: requiring to select IP address or hostname to identify the key;

3) Configure IPSec parameters: including configuring home terminal identification of IP address or hostname, and access-list in order to be quoted in the crypto map;

4) Configure crypto map: creating crypto mapping entries for IPSec, in order to make parts used to establish the IPSec security association coordinate;

5) Apply crypto mapping table to the interface;

6) Configure the tunnel;

7) Apply IPSEC encryption to GRE package;

8) Examine the configuration of IPSec VPN.

B. Networking requirement

A company, with the head office in Beijing, has a filiale in Shanghai. The internal IP of the head office uses class c IP addresses but need to access the Internet. Internal IP addresses can access the company's DNS server and FTP server. Establishment of VPN between sites is called for between the head office in Beijing and the Shanghai filiale. By establishing GRE tunnel, two agencies manage to communicate with each other. Because GRE protocol itself can not encrypt and package the data, we configure IPSec to protect the GRE message.

C. Network topology

The whole network structure is divided into three large blocks, namely Beijing head office networks, Shanghai filiale networks and the Internet. Two enterprise networks are both connected to the Internet network. In order to complete the experiment, the network topology is designed as shown in Figure 1: Router1 is the egress router of Beijing head office, Router 4 is the egress router of the Shanghai filiale, Router2 and Router3 are routers of telecommunication department, and they are used to simulate the Internet network. Terminal equipment are connected in the internal network of the head office in Beijing and Shanghai filiale to test the network connectivity. DNS server and FTP server are placed in the enterprise network.

Experimental topology construction: build a network topology diagram as shown in Figure 1 in the simulation software Cisco Packet Tracer, including four 2811 routers, two 2960 switches, two PCs and four servers.

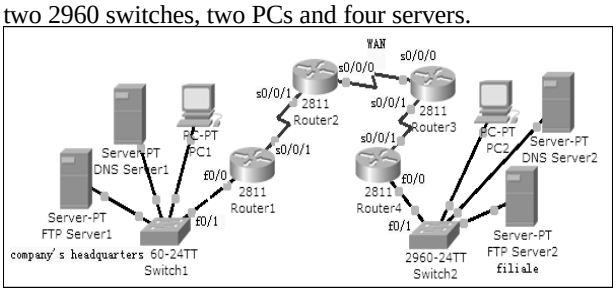

Figure 1. GRE over IPSec VPN net map

D. IP address Configure

When planning IP addresses internal addresses of the Beijing head office are set as Class c IP addresses, 222.17.244.0/24 for Beijing head office and 222.17.245.0/24 for Shanghai filiale. The segment between Beijing head office and the Internet is set to 188.128.5.0/24, and the segment between Shanghai faliale and the Internet is set to 52.1.1.0/24. The network between two external network router is set to 198.96.6.0/24.

Next set IP addresses for terminal machines.

1) Host IP configuration for Beijing head office: IP address of PC1 is set to: 222.17.244.2, subnet mask of PC1 is 255. 255. 255. 0, and the gateway address is set to 222.17. 244.1.

IP address of DNS Server1 is set to: 222.17.244.3, subnet mask of DNS Server1 is 255. 255. 255. 0, and the gateway address is set to 222.17. 244.1.

IP address of FTP Server1 is set to: 222.17.244.4, subnet mask of FTP Server1 is 255. 255. 255. 0, and the gateway address is set to 222.17.244.1.

2) Host IP configuration for Shanghai filiale: IP address of PC2 is set to: 222.17.245.2, subnet mask is 255. 255. 255. 0, and the gateway is 222.17.245.1.

IP address of DNS Server2 is set to: 222.17.245.3, subnet mask is 255. 255. 255. 0, and the gateway is 222.17. 245.1.

IP address of FTP Server2 is set to: 222.17.245.4, subnet mask is 255. 255. 255. 0, and the gateway is 222.17. 245.1.

IV. CONFIGURE ROUTER

A. Configure Router 1

1) Configure IP addresses

```
R1(config)#interface serial0/0/1
R1(config-if)#ip address 188.128.5.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastethernet0/0
R1(config-if)#ip address 222.17.244.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 188.128.5.2
```

2) Establish IKE strategy

```
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#hash md5
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#lifetime 86400
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
```

3) Configure preshared key, and create ACL (IKE parameters)

```
R1(config)#crypto isakmp key 13876694751 address 52.1.1.2
R1(config)#access-list 110 permit ip 222.17.244.0 0.0.0.255 222.17.245.0 0.0.0.255
```

4) Define transform set (IPSec parameters)

```
R1(config)#crypto ipsec transform-set test esp-3des esp-md5-hmac
```

5) Configure crypto mapping table

```
R1(config)#crypto map chong-map 10 ipsec-isakmp
R1(config-crypto-map)#set peer 52.1.1.2
R1(config-crypto-map)#set transform-set test
R1(config-crypto-map)#match address 110
```

6) Apply encrypted mapping table to interfaces

```
R1(config)#interface serial0/0/1
R1(config-if)#crypto map chong-map
```

7) Configure logical interfaces of the tunnel

```
R1(config)#interface tunnel0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#tunnel source serial0/0/1
R1(config-if)#tunnel destination 52.1.1.2
R1(config-if)#exit
R1(config)#access-list 110 permit gre host 188.128.5.1 host 52.1.1.2
```

B. Configure Router 4

1) Configure IP addresses

```
R4(config)#interface serial0/0/1
R4(config-if)#ip address 52.1.1.2 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#interface fastethernet0/0
R4(config-if)#ip address 222.17.245.1 255.255.255.0
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#ip route 0.0.0.0 0.0.0.0 52.1.1.1
```

2) Establish IKE strategy

```
R4(config)#crypto isakmp policy 10
R4(config-isakmp)#hash md5
R4(config-isakmp)#authentication pre-share
R4(config-isakmp)#lifetime 86400
R4(config-isakmp)#group 5
```

3) Configure preshared key, and create ACL

```
R4(config)#crypto isakmp key 13876694751 address 188.128.5.1
R4(config)#access-list 110 permit ip 222.17.245.0 0.0.0.255 222.17.244.0 0.0.0.255
```

4) Define transform set

```
R4(config)#crypto ipsec transform-set test esp-3des esp-md5-hmac
```

5) Configure crypto mapping table

```
R4(config)#crypto map chong-map 10 ipsec-isakmp
R4(config-crypto-map)#set peer 188.128.5.1
R4(config-crypto-map)#set transform-set test
R4(config-crypto-map)#match address 110
```

6) Apply encrypted mapping table to physical interfaces

```
R4(config)#interface serial0/0/1
R4(config-if)#crypto map chong-map
```

7) Configure logical interfaces of the tunnel

```
R4(config-if)#ip add 192.168.1.2 255.255.255.0
R4(config-if)#tunnel source serial0/0/1
R4(config-if)#tunnel destination 188.128.5.1
R4(config-if)#exit
R4(config)#access-list 110 permit gre host 52.1.1.2 host 188.128.5.1
```

C. Simulate WAN-WAN on Router 2 and Router 3 respectively

1) on Router 2

```
Route2(config)#hostname R2
R2(config)#interface serial0/0/0
R2(config-if)#ip add 198.96.6.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial0/0/1
R2(config-if)#ip add 188.128.5.2 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip route 52.1.1.0 255.255.255.0 198.96.6.2
```

2）on Router 3

```
R3(config)# interface serial0/0/0
R3(config-if)#ip add 198.96.6.2 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shut
```

R3(config-if)#exit
R3(config)# interface serial0/0/1
R3(config-if)#ip add 52.1.1.1 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 188.128.5.0 255.255.255.0 198.96.6.1

V. VERIFY THE RESULTS

Wen completed, they can be tested on the client. Use PC1 to ping PC2, namely ping each other between private networks, which theoretically can access, and then ping IP address of analog public network, which doesn't make sense theoretically, testifying that an analog public network just provides a physical link for the tunnel. Input the command on a router 1 to verify the results.

R1#show ip route
C 188.128.5.0 is directly connected, Serial0/0/1
C 192.168.1.0/24 is directly connected, Tunnel0
C 222.17.244.0/24 is directly connected, FastEthernet0/0
S* 0.0.0.0/0 [1/0] via 188.128.5.2
R1#show interface tunnel 0
Tunnel0 is up, line protocol is up (connected)
Hardware is Tunnel
Internet address is 192.168.1.1/24
MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 188.128.5.1 (Serial0/0/1), destination 52.1.1.2
Tunnel protocol/transport GRE/IP

VI. CONCLUSIONS

With the development of modern enterprises, the establishment of branch offices, the formation of remote clients, more and more users need to establish the connection with enterprise Intranet. Combined with GRE, the IPSEC virtual private network (VPNS) can provide enterprises with safe, low-cost and extensible network services without affecting the existing communications. Achieve the real minimum investment and maximum communication. Along with the increasingly important of network security, it can believe that the application of GRE Over IPsec VPN will be more extensive.

REFERENCES

[1] Kang Y K, Kim D W, Kwon T Wet al. An efficient implementation of hash function processor for IPSEC. In Proc. 3rd IEEE Asia-Pacific Conf. ASIC, Taipei, Aug. 6-8, 2002, pp.93-96.

[2] Schaumont P R, Kuo H, Verbauwhede I M. Unlocking the design secrets of a 2.29 Gb/s Rijndael processor. In Proc. 39th ACM/IEEE Design Automation Conference (DAC 2002), USA, June 10-14, 2002, pp.634-639.

[3] Chang H C, Chen C C, Lin C F. XScale hardware acceleration on cryptographic algorithms for IPSec applications. In Proc. International Conference on Inforrnation Technology (ITCC 2005), USA, April 4-6, 2005, pp.592-597.

[4] Grembowski T, Lien R, Gaj K et al. Comparative analysis of the hardware implementations of hash functions sha-1 and sha-512. In Proc. the 5th Int. Information Security Conference, Brazil, September 3-October 2, 2002, pp.75-89.

[5] WANG C, Lo C, Lee M, et al. A network security processor design based on an integrated SoC design and test platform [C]//Proc. IEEE/ACM Design Automation Conf. (DAC'06), IEEE Press, 2006:490-495.

[6] China Core C * Core310 User Guide [R]. ChinaCore Inc. [EB/OL]. (2004). http: //www. china-core, corn/data/ summary/C310_datasheet chinese, pdf.

[7] WANG Haixin, BAI Guoqiang, CHEN Hongyi. Zodiac: system architecture implementation of a high performance network seeurity processor [C]// Proc IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP'08), IEEE Press, 2008:91 - 96.

[8] Verbauwhede I, Scheaumont P, Kuo H. Design and performance testing of a 2.29 Gb/s Rijndael processor [J]. IEEE Journal of Solid-State Circuits, 2002, 28(3): 569 - 572.

[9] CHEN Gang, BAI Gguoqiang, CHEN Hongyi. A high-performance elliptic curve cryptographic processor for general curves over GF(p) based on a systolic arithmetic unit [J]. IEEE Transactions on Circuits and Systems II-express briefs, 2007, 54(5): 412-416.

[10] Chou W. Inside SSL: accelerating secure transactions [J]. IT Professional, 2002, 4(5) : 37 - 41.

[11] Onuki A, Takeuchi K, Inada T et al. A realization of theoretical maximum performance in IPSec on gigabit Ethernet. IEEJ Transactions on Electronics, Information and Systems, 2004, 124-C(8): 1533-1537.

[12] Dandalis A, Prasanna V K, Rolim J D P. An adaptive cryptographic engine for IPSec architectures. In Proc. IEEE Symposium on Field-Programmable Custom Computing Machines, USA, April 17-19, 2000, pp.132-141.

[13] Castanier F, Ferrante A, Piuri V. A packet scheduling algorithm for IPSec multi-accelerator based systems. In Proc. the 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP 2004), USA, Sept. 27-29, 2004, pp.387-397.

[14] Niemann J G, Porrmann M, Ruckert U. A scalable parallel SoC architecture for network processors. In Proe. IEEE Computer Society Annual Symposium on VLSI 2005 (ISVLSI 2005): New Frontiers in VLSI Design, USA, May 11-12, 2005, pp.311-313.

[15] Ariga S, Nagahashi K, Minami M et al. Performance evaluation of data transmission using IPSec over IPv6 networks. In Proc. INET 2000, Yokohama, Japan, USA, July 18-21, 2000, pp.200-202.

[16] Caldera J, Niz D D, Nakagawa J. Performance analysis of IPSec and IKE for mobile IP on wireless environments. Information Networking Institute, Carnegie Mellon University, http://www.cs.cmu.edu/-dionisio/ipSec-wmip.doc.

[17] Elkeelany O, Matalgah M M, Sheikh K Pet al. Performance analysis of IPSec protocol: Encryption and authentication. In Proc. IEEE International Conference on Communications (ICC 2002), New York, USA, April-May, 2002, pp.1164-1168.

[18] Kent S, Atkinson R. Security architecture for the Internet protocol. RFC 2401, November 1998.

[19] Kent S, Atkinson R. Security architecture for the Internet protocol. RFC 4301, December, 2005.

[20] Madson C, Glenn R. The use of HMAC-MD5-96 within ESP and AH. RFC 2403, November 1998.

[21] Madson C, Glenn R. The use of HMAC-SHA-1-96 within ESP and AH. RFC 2404, November 1998.

[22] Madson C, Doraswamy N. The ESP DES-CBC cipher algorithm with explicit IV. RFC 2405, November 1998