Improvements based on the IPSec VPN Secuirity

Ya-qin Fan, Ling Lv, Mei-lin Liu, Fei Xie
College of Communication. Engineering, Jilin University
Changchun 130012, china
Zhangnan9970@126.com

***Abstract*—In this paper, through specific description of the concept of virtual private network VPN, operating principles and the IPSec protocol, and using the OPNET software for performance simulation of IPSec VPN network, we get the result of IPSec VPN throughput of the network, which is unstable. o though IPSec VPN has improved the safety performance of data transmission, it at the same time affects the transmission efficiency. By analyzing the problems of IPSec VPN, in terms of improving safety performance, the combination of PKI and IPSec VPN program was proposed. Theoretical analysis shows that such program can indeed solve the problem of authentication imperfect, thus improving the safety performance of the network.**

Key words-Virtual Private Network IPSec protocol security

I. OVERVIEW

A. VPN Technology

VPN is Virtual Private Network, the open public network as the user information transmission platform, at the same time through the tunnel encapsulation, data encryption, user authentication and access control technology to realize the transmission of data security protection, so users can enjoy similar special security performance of the network. In general, according to the needs of enterprises to organize their own local area network, because the IP shortage, its internal IP always uses the reserved address. But due to the retention of the address on the Internet cannot be routed, so we often cannot be directly accessed by the Internet located in the internal LAN host. In this case, the VPN tunnel technology emerge as the times require[1-2].

B. IPSec Protocol

The basic idea of IPSec is in the IP protocol introduced can protect data security mechanism. The use of modern advanced cryptography methods for carrying authentication and encryption type service type service. This move so that the user can according to the important degree of data to select their own to achieve the desired security services[3]. The IPSec data information provides interoperability, high quality, based on modern cryptography security protection mechanism. As a result, under certain conditions, specific to communicate with each other two party users can in IP layer, through the data source authentication and encryption methods, in order to guarantee the transmission on the network reported data integrity, privacy, and playback and real.

II. OPNET ENVIRONMENT VPN MODEL

In the OPNET simulation software in 11.5, virtual private network VPN model as shown in Figure 1 below:

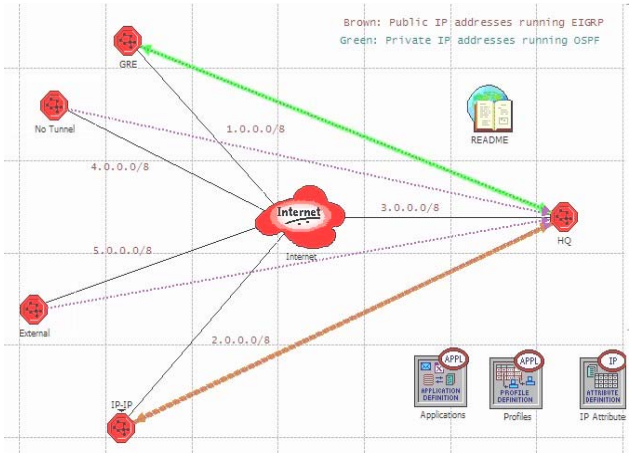


Figure 1 the VPN s_ with_ IP_ Tunnels model

The model is an enterprise global network of each site construction model and composition. The following is the network model specification:

① HQ: this node module represents the headquarters.

② GRE: this node module for a remote VPN site.

③ IP-IP: this is another remote VPN site.

④ No Tunnel: which is internally using private IP address to the site, but it cannot connect to HQ site.

⑤ External: this node module is running the EIGRP protocol and is using public IP address. And this node can communicate with the HQ site " External " nodes are connected to each other[4-5].

The Internet: This is a network, but the network is composed of a plurality of running the EIGRP protocol router constructed. This one of the nodes in the network in the simulation needs to be disconnected, in order to test the effect of tunnel on and off[6].

Published by Atlantis Press, Paris, France.

III. OPNET IPSEC UNDER THE ENVIRONMENT OF VPN PERFORMANCE TESTING

A. *To Establish the Network Topology Structure*

The IPSec VPN Windows simulation in XP environment, OPNET11.5 simulation platform, the first to establish the network topology structure diagram as shown in figure 2:

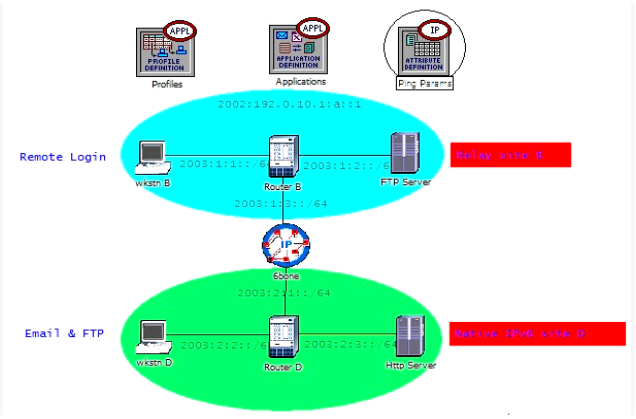


Figure.2 Simulation topology map

From the above shown in the topology map, can be seen, in this system, it is configured with two clients, namely wkstnB and WkstnD; configuration of the two router, namely RouterB and RouterD; at the same time also configured two server, FTP server and Http server; finally a pure IPv6 Internet 6bone configuration in RouterB and RouterD intermediate.

B. *The Nodes of the Model Service Parameter Configuration*

①Applications Definitions configuration: on the node configuration of the FTP Applications, Web Applications, Email Applications, Remote Login Applications and Voice Applications five application.

②Ping Params configuration: system for this node configuration for IP Ping Parameters as follows: Defult respectively (Ipv4); Record router (Ipv4); Defult (Ipv6) and Record router (Ipv6).The Profiles attribute is defined as shown in Figure 3 below:

- Applications	(. .)
├rows	2
- row 0	
├Name	Web Application
├Start Time Offset (s...	uniform (5, 10)
├Duration (seconds)	End of Profile
Repeatability	(. .)
├Inter-repetition T...	exponential (300)
├Number of Repetitions	constant (0)
└Repetition Pattern	Serial

Figure.3 on the Profiles attribute definition

On the configuration of Profiles, defines the start time Start time:uniform (5,10); duration (Duration): end of Profile; reproducibility (Repeatability): exponential (300), constant (0), Serial. The configuration of the router B and router D between VPN channel. In the configuration, the definition of VPN channel starting point (D router) and the end (B router), VPN delay: constant (0), operation system (Operation Mode): Compulsory, the remote client: wkstnD.

C. *The Topology of the IPv6 Configuration Parameters*

On the topology of the IPv6 configuration parameters, such as shown in Figure 4 below:

- row 1	
├Name	IF10
├Link-Local Address	Default EUI-64
Global Address(es)	(. .)
├rows	1
+ row 0	2003:1:2::1,64, Non EUI-64
├Routing Protocol(s)	RIPng
+ Neighbor Discovery P...	Default

Figure.4 IPv6 topology configuration parameters

The simulation experiment is divided into two scenes on the nodes of the network parameter configuration. The first scene is supposed to be pure IPv6 under the environment of network node configuration, this time without setting up an VPN connection. In the second scene needed to configure the IPv6 environment is under IPSec VPN. In pure IPv6 environment, the RouterB configuration for:

The LINK-LOCAL ADDRESS is set to DEFAULT, the ROUTING PROTOCAL routing strategy is set to PING, at the same time, each node address set out.

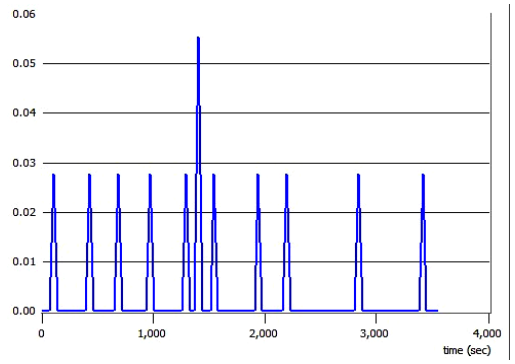
D. *IPSec Network Model of the Specific Configuration*

The simulation on the scene only configuration IPv6 environment simple network, second scenes in the IPv6 environment settings for IPSec VPN. For the IPSec parameter is set to: authentication algorithm is set to MD5; the authentication method is set to Preshared Key; the encryption algorithm is set to 3DES; Lifttime 86400; DH Group is set to Group1; IPSc policy settings for ESP; authentication algorithm is set to HMAC, MD5 will be set to 3DES; encryption algorithm. Set after the IPSec and VPN are configured on the scene, named IPv6-IPSec-vpn[7-9].

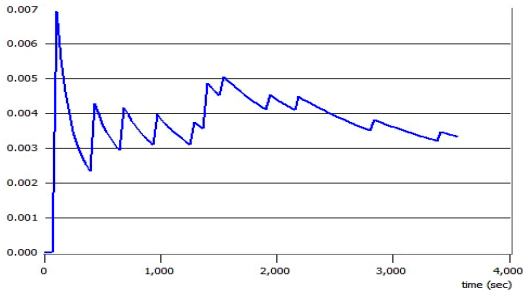
IV. RESULTS OF SIMULATION ANALYSIS

Simulation time of 60 minutes, run on a computer simulation of the time to 13 seconds. In Scene 1, the throughput of FTP.Server as shown in figure 5:

Through the analysis and comparison of figure 2 and figure 3 of the simulation results, we can easily draw the following conclusion: in two scenarios of FTP server



Scene 1 (a) FTP.Server throughput (As Is)



Scene 1 (b) FTP.Server throughput (average value)

Fig 5Scene 1 simulation results

In Scene 2, the throughput of FTP.Server is as shown in figure6:

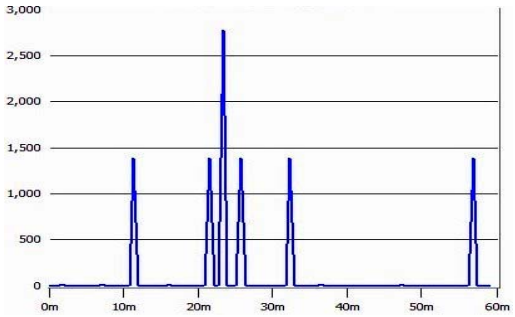


Fig. 6 (a) scene 2 FTP.Server throughput (As Is)

throughput is not smooth, changing. But obviously, set the IPSec VPN IPv6 network FTP server throughput fluctuation is more serious, and the scene one more unstable. Thus we can draw a conclusion that, although the IPSec set up the VPN network's security performance are significantly improved, but it will greatly reduce the transmission performance of the network, the influences of network quality of service. This is because the IPSec

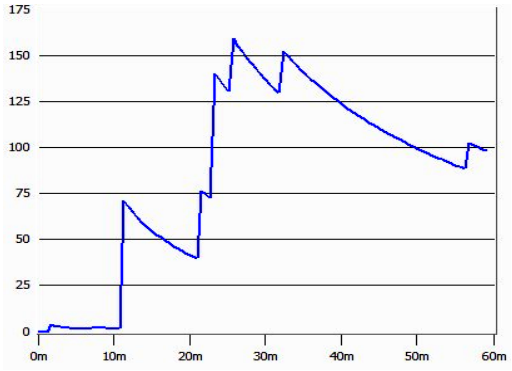


Fig.6 (b) scene two FTP.Server throughput (average value)

Fig 6 Scene 2 simulation results

based VPN was used in the tunnel encapsulation technology, to ensure the safety at the same time also must sacrifice some properties. Therefore, we can learn: transmission efficiency and safety are mutually contradictory, in the application of it in different network environment and performance needs to select the corresponding configuration.

V. IMPROVEMENTS BASED ON THE IPSEC VPN SECUIRITY

Although, based on the IPSec VPN has greatly improved the network's security performance, but inevitably there are still certain safety factor. The unsafe factors exist in the transmission path ends. For example, if the hackers to attack the enterprise internal network application system, once the remote user and enterprise internal network to the IPSec VPN way to build online, the internal network application system will be hackers are detected, the enterprise's internal data is facing greater security risk. To solve this problem, we can design the key infrastructure PKI and IPSec VPN combination scheme can improve the identification, the problems of imperfect, effectively improve the security of network, to make IPSec security is improved, and the development of.

A. PKI System Introduced

Key infrastructure PKI is a kind of follow the established criteria for the key management platform, able to basically all network provides digital signature and data encryption of the password, and the network needs the certificate and key management system. From this point of view, it can just make up for the IPSec identity authentication in the imperfect aspects of deficiency.

VPN as a network security services, the need to combine the performance of PKI mainly has the following three kinds: identity authentication; key management; access control.

B. Based on the PKI IPSec VPN Applications Model

In the IPSec VPN in the application of PKI model as shown in figure 7:

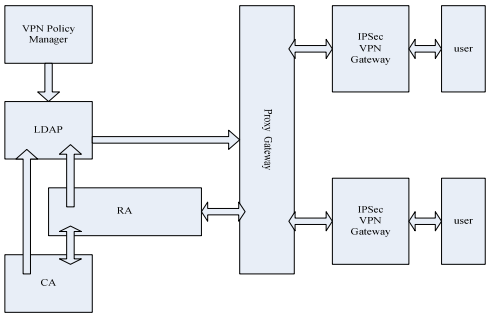


Figure.7 IPSec VPN, application of PKI model

User A and user B to VPN communication as an example to illustrate the above operation steps:

(1) to the first communication of both A and B through the proxy PKI gateway in LDAP gets its own identity certification;

(2) by VPN Policy Manager

Awarded attribute certificate, the certificate decision is whether to allow the user to set up the virtual connection A and B communication;

(3) the user A and B will each certificate to each other, each identified by CA with each other if the communication is safe, the presence or absence of risk;

(4) system to check the certificate revocation list CRL, as long as the A or B has a certificate in the list, then we can determine the party's certificate has expired, the connection failed;

(5) if CA certificate and attribute certificates are verified, will be able to successfully establish a connection, or as long as one is not verified, that access permissions, the connection failed.

In this scheme, the system security is strengthened, firstly because of the CA for each user certificate is the only, and does not normally change. In the scheme, the user's identity is IP addresses to identify, but IP addresses may be with the site or service providers change. Because of the digital certificate does not change, therefore enhances the identity and uniqueness. Naturally, will enhance the security of. Secondly, because the VPN gateway and PKI direct communication, but through the PKI proxy gateway indirectly communicating with PKI. The communication on the other side of a domain name or address is sent to the proxy gateway, proxy gateway into the PKI system information and obtain the corresponding certificate, the certificate will be obtained after once again verify and assert, in order to decide whether to allow the connection establishment. Therefore, it not only effectively enhances the system processing business ability, also strengthened the communication security and reliability.

VI. HEAD NODE

With the rapid development of Internet, network security has been paid more and more attention, VPN (virtual private network) makes application of unsafe in the public network transmission encryption information becomes possible. This paper in the VPN and IPSec protocol is introduced, based on the IPSec VPN throughput and delay index made simulation. Through the simulation data, we can understand the IPSec based on VPN impact on network performance. Now the VPN technology based on IPSec in some of the problems put forward an improved scheme. To key infrastructure PKI and IPSec VPN combination scheme can improve the identification, the problems of imperfect, effectively improve the security of network, to make IPSec security is improved, and the development of. Put forward a proposal, in theory of the scheme is analyzed, the scheme is proved in theory, in a way to improve network security, improve the internal network security performance.

REFERENCE

[1] Chen Juan, Wei Yiliang IPSec. Based on the security of VPN data hybrid encryption algorithm .[J]. railway computer application 2009,19 (3): 88-92

[2] Yang Tao PKI IPSec-VPN. Combining with the design and implementation of.[J]. monitoring and control technology of 2009,28 (9): 92-96

[3] Liu Huachun PKI based research and design of IPSec-VPN .[J]. communication technology 2009,01 (42): 258-262

[4] Li Rongsen, Qin Jie. The embedded PKI simulation software platform for the design and implementation of.[J]. Computer Engineering, 2007,33 (16): 108-112

[5] Qian Yan, Zhang Jifeng.IPSec VPN gateway in IKE communication system design .[J]. science and technology 2008,8 (4): 55-59

[6]. Based on OPNET IPSec VPN performance analysis .[J]. communication technology 2009,09 (42): 88-92

[7] Huang Xiaogang mobile IPSec VPN implementation method of improving performance of .[J]. Computer Security 2009, 5 (2): 10-12

[8] Zhou Yongbin.IPSec VPN safety .[M]. Beijing: Tsinghua University press, 2007:240-300

[9] Chen and .Linux operating system kernel analysis.[M]. Beijing: Publishing House of electronics industry, 2006:180-250