The Design and Realization of the Test Scheme OpenVPN, Based on Message Simulation

Hou Zhan-sheng, Xu Min, Zhu Li-peng, Peng Lin, Hu Bin
Research Institute of Information Technology & Communication
China Electric Power Research Institute
Nanjing, China
houzhansheng@epri.sgcc.com.cn

***Abstract*—This paper studied the SSL protocol and the principle of OpenVPN, proposed a hardware-based encryption access system OpenVPN, which drawn the block diagram of design structure, In view of the problem of OpenVPN concurrent test, general concurrent test based on the recording and playback mechanism, constitute a single process, by recording and playback process. However, the OpenVPN access system based on SSL protocol, the encryption protocol security design, especially hardware encryption packet not be copied features, proposed a concurrent test scheme which based on IP message simulation and solved the problem of OpenVPN access system concurrent test, which provided a good inspiration for the next step more in-depth study.**

Keywords- Virtual Private Network, SSL protocol, OpenVPN, Recording and Playback, Concurrent test

I. INTRODUCTION

VPN (Virtual Private Network) is physically located in different areas in the backbone network through a public network connected to the logic of a virtual subnet. SSL (Secure Sockets Layer) protocol [1] is a kind of secure channel between two devices provide network security protocol, It uses data encryption, authentication, tunneling [5], key management and other key technical support data transmission security. OpenVPN [2] is based on the SSL protocol open source software, this article based on the OpenVPN software designed a hardware-based encryption and decryption of access systems.

General concurrent test [9] based on recording and playback mechanism, which through constitute a single process by recording, and then through multiple processes/threads playback process method. However, OpenVPN SSL protocol based access system, because encryption protocol [8] own security design, In particular, the server and the client when using hardware encryption and decryption, encrypted data packet can not be copied properties, therefore, recording and playback can not be used for concurrent test manner. Based on this, this article presents a simulation based on IP packet of concurrent test methods.

II. OPENVPN IMPLEMENTATION PRINCIPLES

OpenVPN is SSL-based VPN protocol of open source software, its technical core is a virtual NIC [2] and SSL/TLS protocol [3] to implement, and provides a variety of authentication methods to confirm the identity of the parties involved in connecting, including: pre-enjoy private, third-party certificates, username/password combination [1], but also has powerful ACL function [6] restrict customer information exchange. OpenVPN uses the OpenSSL library to encrypt data and control information, the use of the OpenSSL encryption and authentication features, it can use any OpenSSL support algorithm. In addition, OpenVPN via PKCS#11 support hardware encryption identification, such as smart cards (PCI encryption card, USB/TF card encryption).

OpenVPN work of the OSI model 2 or 3 layers, using TUN/TAP driver [7] implements virtual NIC functionality. Through the use of application-layer SSL/TLS protocol tunneling encrypted transmission function, with good security and scalability [4], as well as providing fine-grained access control [6]. Which, TAP is equivalent to an Ethernet device, which operates the second layer packets (eg: Ethernet data frames), TUN simulated network layer devices, operating the third layer packet (eg: IP data packets). OpenVPN via TUN/TAP device to bind the device's user-space programs to send data, at the same time, user-space programs can also operate the hardware network devices such as through the TUN/TAP device sends data.

The work is divided into OpenVPN routing mode and bridging mode, the main difference is: in the routing mode, VPN IP broadcast packets are not transmitted in bridge mode, VPN IP broadcast packets transmitted, which is generally more common routing mode.

Process of sending data: (1) local application to a virtual private network range of IP addresses to send network packets, (2) network packets according to the routing table to route data to the virtual network card, (3) virtual network adapter to put the data in the data queue, the queue character device reads the data in the data sent to the application layer, (4) OpenVPN process will use this packet tunneling protocol encapsulation and encryption via physical NIC to the virtual private network each node.

Receive data process:(1) physical NIC to accept encrypted IP packet, the packet will be transmitted to the user space, (2) OpenVPN process will decrypt the encrypted IP packet, the character device to pass through the virtual network card, (3) the decrypted data through the virtual network card to re-enter the network stack, network stack the data to the upper real application.

OpenVPN bridge mode works as follows:

Process of sending data:(1) local application to send data inwards network segment, (2) Data is automatically added by the OpenVPN client's (server-side push over, and the virtual network itself) routing rules route to the virtual network

adapter, (3) virtual network adapter to put the data in the data queue, (4) OpenVPN process provided through a virtual character device interface card reads IP packet, (5)OpenVPN process encrypted IP packets and sent through the physical NIC to the peer.

Receive data process:(1) OpenVPN process from the physical NIC receive encrypted messages, decryption, and through the virtual device interface card provides a character written to the virtual network adapter, (2) virtual network adapter IP packets into the network protocol stack for processing, restore a virtual NIC on the incoming data, (3) data through the machine iptables rules such as routing and forwarding to the intranet server.

III. OPENVPN SYSTEM DESIGN

OpenVPN access communication module is the core of the system used to complete the application packet capture, encryption, and forwarding. The module is based on OpenVPN open source software secondary development completed, shown in Figure 1.

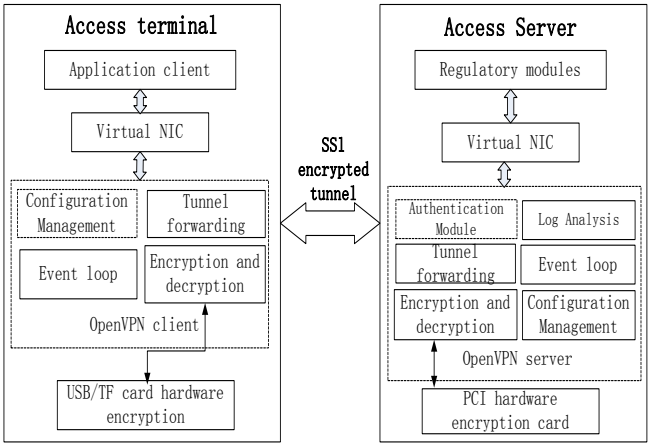

Figure 1. System Block Diagram Functional Design

The terminal and the access client, respectively, to achieve OpenVPN client and server program module function. The client and server in the process of establishing an encrypted tunnel using SSL transport protocol. Among them, the client and the access server hardware encryption using calling cards using encryption operations. To mask the differences between the hardware required to achieve independent of specific hardware encryption transparent encryption engine. On the RSA asymmetric algorithms, SM1 symmetric algorithm [1] respectively to achieve, using the open source OpenSSL [7] provides cryptographic engine architecture for secondary development package. Client Encryption hardware with built-State Encryption Administration SM1 symmetric algorithm security USB / TF encryption card interface via CSP package asymmetric algorithms RSA function, Engine package [8] to achieve SM1 algorithm calls. Server hardware using RSA asymmetric encryption algorithm chips, SM1 symmetric encryption algorithm chip PCI card for RSA asymmetric algorithms, SM1 symmetric algorithms take Engine encapsulation mechanisms.

IV. OPENVPNCONCURRENT TEST DESIGN

OpenVPN application data transmission system based on virtual private channel, that VPN technology, the access system using the State Encryption Administration SM1 specified cryptographic algorithm, which is a non-disclosure of the algorithm, only the hardware implementation. Terminal software must be USB / TF card encryption and decryption operations. Therefore, the use of actual hardware (eg: 5000 terminals) to large-scale concurrent, The test is unrealistic, which requires massive simulated client [9] for large-scale concurrent testing.

A. concurrent test the technical difficulties

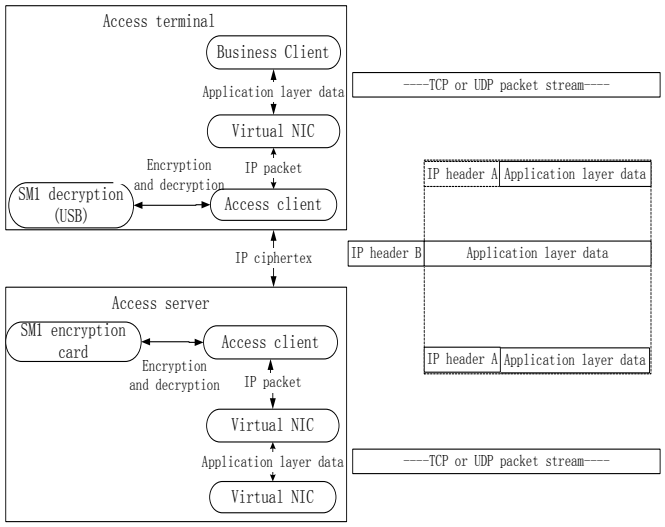

Figure 2. Flowchart real terminal access gateway

Figure 2 analyzes the real terminal access gateway and forwards the data to business processes. When the client after successful access gateway will start the virtual NIC; virtual card capture application layer data, and in the form of an incoming IP packet access clients; access client using the SM1 encryption card is encrypted IP packets, generates an encrypted IP packets and sent to the access gateway; access gateway decrypts the encryption card through SM1, get plaintext IP packets, and writes the virtual NIC, revert to the original business data, and then pass back-office business services.

Business data forwarding process and request data is forwarded to the contrary. Access Gateway through a virtual business card to get the response data, then send encrypted access client; client decrypted and written to the virtual card, revert to the original business data, and ultimately passed to the business client software.

Single terminal access gateway test is feasible to simulate large-scale concurrent client mass tests, but the following technical difficulties:

1) Access clients rely virtual NIC for IP packet forwarding, virtual card only supports a single process, single thread, and the same machine can be installed in a limited number.

2) Access terminal using SM1 (USB/TF) encryption card supports only single-process, single-threaded simultaneous calls, and a limited number of encryption card SM1.

3) Because the encryption protocol security requirements, in any two between the client and server to negotiate the encryption key is different, that is, the same set of application data sent from the client to the server A, and B sent from the client to the server, encrypted transmission in the channel content is different. If a way of recording and playback, the second terminal from a data packet capture channel and other channels will not be recognized by the server.

B. Design of concurrent test

To solve the above technical difficulties, to achieve the same test equipment to run multiple clients for testing, need to separately access client and the virtual NIC module SM1 decryption module adapted accordingly, be designed to be tested test client, thereby performing the concurrent test.

First, clients access the virtual NIC module transformation. After removing the virtual network adapter module, the access client is no way to get real business data, the client must access their business data to generate simulated. Meanwhile, in order to simplify the following encryption solution for SM1 module simulation, the simulation generated business data must be kept simple fixed, while the number and size of its packets controllable. Taking these requirements, simulation data generated by business decision ICMP request packets, in which the only variable is the access client is assigned to the virtual network adapter IP address (Source Address).

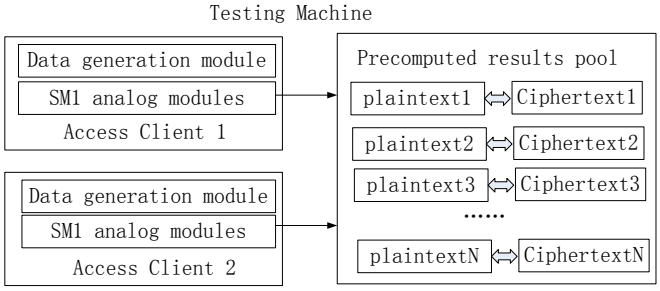

Figure 3. Analog SM1 operations to generate IP packets

Then, transformation for encryption module SM1, Since currently only SM1 symmetric algorithm implemented in hardware, so the algorithm for simulation, can take a fixed key, and all possible input calculated in advance (that is, IP packet service data) calculation results, shown in Figure 3, according to the data generation module generates all possible IP packets, pre-computed results SM1 encryption and two-way mappings. Data encryption and decryption operations in the simulation process directly to the bidirectional mapping table to find the corresponding value, thus completing the simulation generates business data.

Completion of the two parts of the transformation, the resulting test client to the virtual NIC and in the absence of the two modules SM1 encryption card, under the premise of the access and data transmission services to simulate the process, and can be on the same test equipment to run multiple client software such tests, when the test client successfully access gateway, began to generate business data corresponding analog IP packets, and then check the results of pre-computed, the IP packet is encrypted and send to access Gateway; access gateway is the same as the real access gateway through SM1 decrypt encryption card, get plaintext IP packets, and writes the virtual NIC, revert to the original business data.

Since the business data is the ICMP request packets, so the stack gateway system will automatically generate a corresponding ICMP response packets and sent through the virtual NIC Access Gateway; access gateway encrypts send test client after ; the test client via reverse lookup pre-computed results are obtained plaintext response message, and then outputs the corresponding test information, test results for statistical purposes.

Eventually, the client machine to run multiple simulations access client, the client successfully connected through the number to calculate the maximum number of concurrent connections, gateway virtual NIC by detecting network traffic throughput computing access gateway, access gateway and the client under contract to calculate the number of packets received and transmitted packet loss rate.

V. ANALYSIS OF TEST RESULTS

The program tests a single access gateway (single), two access gateway Load Balancing (double) in case of the maximum number of concurrent connections, throughput, packet loss rate transmission.

LVS cluster [10] using IP load balancing technology and content-based request distribution technology, mainly to support three network modes: NAT, DR, and Tunnel. Where load balancing technology uses NAT mode, it NAT gateway / firewall functionality is similar to the network for packet forwarding address translation, and then in two segments inside and outside the exchange of packets between. And NAT gateway / firewall is different, LVS load according to the configured rules will come from different clients connected network packets forwarded to different servers through dynamic allocation algorithm for processing, and to ensure the connection with a the packet is forwarded to the same server.

Among them, the client machine simulation, access gateway A, access gateway B, contracting servers use Gigabit Ethernet, in order to exclude the throughput bottleneck switches cause interference to flow test, where two switches are used gigabit switches. Meanwhile, in a real version is installed on a PC client, as a client of the N +1 independent testing.

1) The maximum number of concurrent connections

Maximum number of concurrent connections: a single access gateway to withstand the maximum number of

terminal access, the two gateways in the load balancing condition to withstand the maximum number of terminal access, shown in Figure 4.

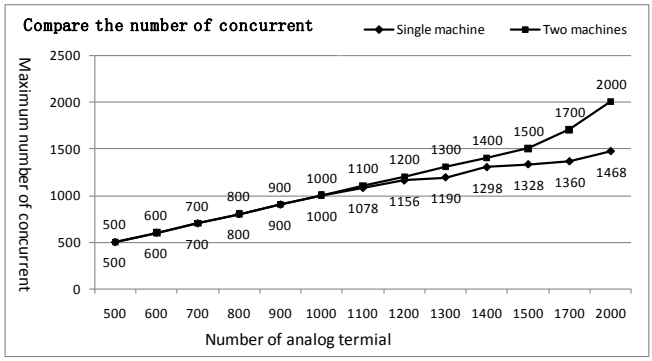

Figure 4. Single and double the maximum number of concurrent connections contrast

2) Throughput

Throughput: access gateway to upload or download transfer rate and its relationship with the relationship between the number of terminals. Used here each simulated client upload traffic 0.3Mbs, the test and two single gateway load balancing throughput under comparison, shown in Figure 5.

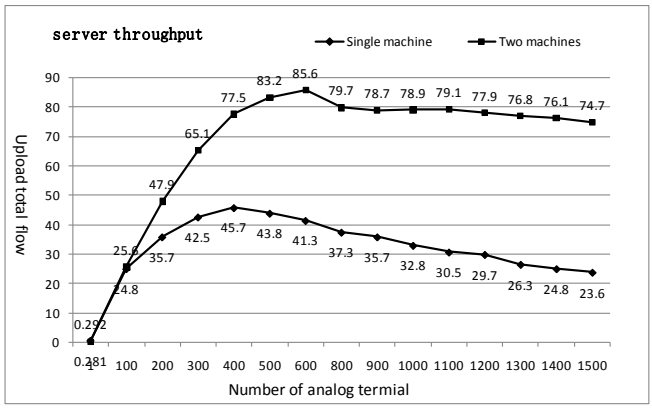

Figure 5. single and double contrast gateway throughput

3) Transfer the packet loss rate

Transmission loss rate: secure access gateway and the analog transmission of data between the client, the actual received data packets and the ratio between the theoretical number of sent packets, shown in Figure 6, Single machine and two machines, in the case of load balancing, packet loss rate when uploading 1Mbs.

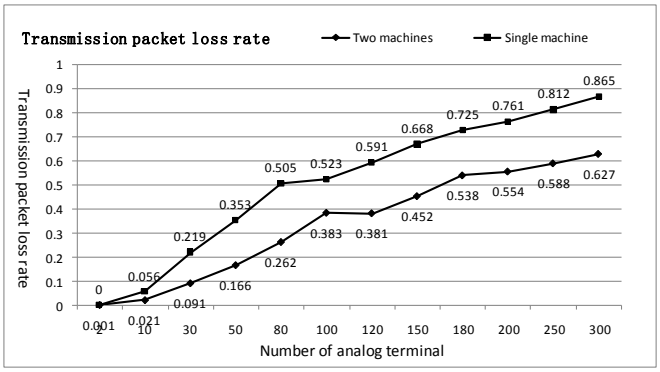

Figure 6. single and double contrast transmission packet loss rate

VI. CONCLUSION

This paper designed a hardware-based encryption OpenVPN access system, to achieve data encryption, authentication, secure transmission tunnel, as well as client permissions for effective control to prevent unauthorized users from illegal access and other functions, especially for OpenVPN concurrent test can not be tested using the general concurrent recording and playback mechanism is designed based on IP packets concurrent simulation testing program, OpenVPN has solved the problem of concurrent test access system, this design has a more unique ideas, more in-depth research for the next provides a good source of inspiration.

[1] SSL VPN Technology Specification. State Encryption Administration, 2009.01:5-31.

[2] Markus Feilner. OpenVPN: Building and Integrating Virtual Private Networks.Birmingham:Packt Publishing Ltd. 2006:167-186.

[3] Guo Ling, LI Wei-sheng. SSL VPN Design and Implementation of Computer Technology and Development, 2007.08, Volume 17 8 :148-150.

[4] YU Sheng-sheng, Wang Yong. LINUX under a secure SSL VPN Design and Research of Computer Engineering and Science, 2006.01, 28 No. 1 :1-2.

[5] Han Wei, Xue Jian, Bai Ling. Based on tunneling technology SSLVPN security and performance analysis. Science Technology and Engineering, 2005,5 (12) :791-795.

[6] Guo Xue-chao, ZHAI Zheng-jun. OpenVPN System Security Research Science Technology and Engineering, 2007.04, Volume 7, 8 :1742 -1745.

[7] Eric Reseorla. Cui Kai translation. SSL and TLS: Designing and Building Secure Systems [M]. Beijing: China Electric Power Press,2002.03:11-38.

[8] Bruce Schneier. Wu Shizhong, Zhu Shixiong such as translation. Applied Cryptography - Protocols, Algorithms and C source code. Machinery Industry Press,2007.09:33 -45.

[9] Zhu Shaomin. Software testing methods and techniques. Beijing: Tsinghua University Press,2005:23-34.

[10] Li Wei. Software test automation framework for Research and Implementation of Hybrid: master's degree thesis. Beijing: Beijing Jiaotong University,2007:28 -45.