Hardware-and-Software-Based Security Architecture for Broadband Router (Short Paper)*

Gu Xiaozhuo [1,2,3], Li Yufeng[1,3], Yang Jianzu [3], and Lan Julong[1,3]

[1] National Digital Switching System Engineering & Technological R&D Center, China
[2] Lanzhou City College, China
[3] Information Engineering University, China
No 783 Po Box 1001, 450002, Henan, China
{gxz, lyf}@mail.ndsc.com.cn, yjzxxgc@sohu.com,
ljl@mail.ndsc.com.cn

Abstract. Implementing IP security in broadband router without sacrificing the performance is main work we focused on. To meet the need of protecting wire speed forwarding data passing through fast path of the router, security module implemented with encryption chip was adopted; to protect non real time data passing through slow path of the router, the scheme of implementing IP security inside kernel of Master control module with software was introduced. Security architecture and several testing architectures were finely designed and depicted in the paper. Testing of security architecture was undergone in SR1880s router, which was developed by National Digital Switching System Engineering & Technological R&D Center of China (NDSC). Testing results show that the two schemes work well together.

Keywords: IP security (IPsec), Security architecture, Security module, IPsec module.

1 Introduction

With fast development of Next Generation Internet (NGI), routers are required to support IPsec as essential function. Owning to relatively mature technology of router manufacture, implementing IPsec in routers without changing the original framework is the recent work being focused on.

General security architecture shown in Fig. 1 has two main disadvantages. First, each Network processing unit with one Encryption chip will lead every packet passing through Network processing unit also passing Encryption chip, yet there is small part of traffic that needs to be protected by Encryption chip. Second, N Encryption chips together will aggravate the problems of power waste, heat dissipation, and electromagnetic compatibility in single-shelf

Comparing with the general security architecture, we put forward universal security architecture and adopted it in SR1880 series to make the testing. SR1880

* This work was supported by the National High Technology Research and Development Program of China (No. 2005AA121210).

P. Ning, S. Qing, and N. Li (Eds.): ICICS 2006, LNCS 4307, pp. 546 – 555, 2006.

series has breakthrough in system architecture of router, high-speed forwarding engine [4][6], switch fabric, and scheduling algorithm [5]. All of these innovations have been implemented successfully in SR1880 series routers. We designed universal security architecture and implemented it in SR1880 series, which are called SR1880s.

We will introduce system architecture of SR1880s router in section II, and discuss designing and implementing of IPsec in SR1880 series in section III. Section IV will present several test architectures for testing and section V will give the conclusion.

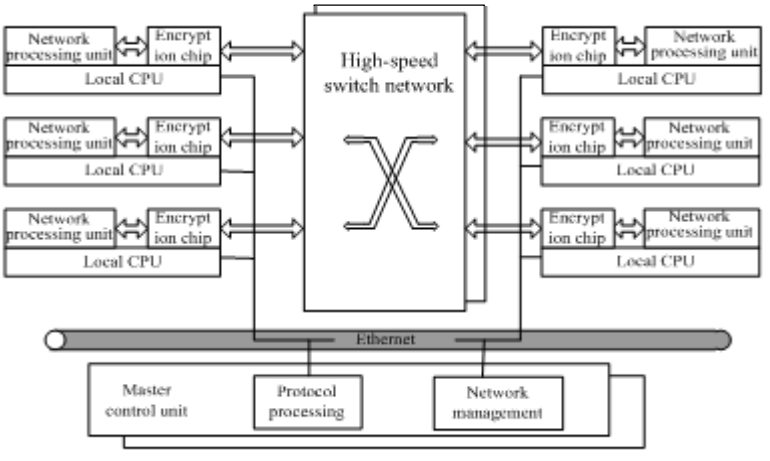

Fig. 1. General security architecture of broadband router

2 System Architecture of SR1880S

SR1880s router adopts decentralized module architecture shown in Fig. 2. Totally there are six main modules of the router, which are Line card interface module, Forwarding module, Photonic switching network, Security module, Inner communication module and Master control module.

Line card interface module includes 2.5G Packet over SONET/SDH (POS) interface, 155M Asynchronous Transfer Mode (ATM) interface and Gigabit Ethernet interface to process the packet in layer 1 and layer 2. Forwarding module is designed to forward the packet in layer 3, including wire speed forwarding, filtering and security checking, classification according to priority, identification of multicast and tagging, and inner packet forming. Photonic switching network provides service of exchanging packet according to different operation levels. Security module performs encryption and decryption of inbound and outbound packets. Master control module manages routing calculation, network management, device configuration and control, and IPsec module inside kernel. Inner communication module is the hinge to complete exchanges between every function board and Master control module.

Security module is consisted of Encryption adaptive board with dynamic Encryption chips to avoid the problems existed in general security architecture of the router. Security module is an independent part which has two outer interfaces, one is with Photonic switching network and the other is with Master control module. The

number of Encryption chips in one Encryption adaptive board is changeable according to anticipated traffic passing through router. When one adaptive board full loaded can not meet the need, more Encryption adaptive boards can be added.

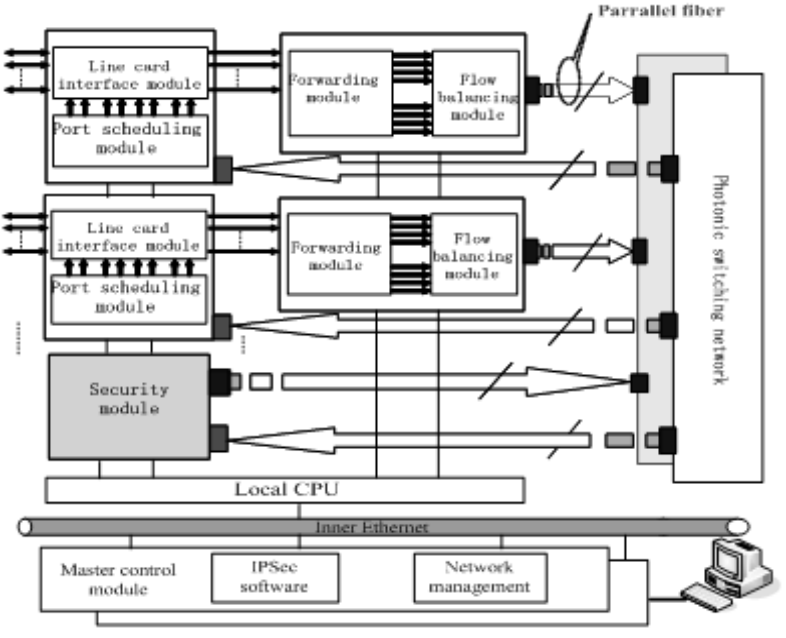

Fig. 2. System Architecture of SR1880s

3 Security Architecture of SR1880S

The architecture of SR1880S can be partitioned into two planes, data plane (fast path) and control plane (slow path), according to the design of separating the routing and forwarding data. Forwarding data are processed and forwarded in high speed through Line card interface module, Forwarding module, and Photonic switching network. In slow path, Master control module, Inner communication module, and local CPU cooperate together to fulfill the maintenance, control and management of the router through processing non-real time tasks. To provide protection for entire traffic passing through router, we put forward two schemes of implementing IPsec working together. One scheme uses hardware to process high-speed forwarding data in fast path, and the other scheme uses software inside Master control module to process non-real time data in slow path.

3.1 Security Architecture of Implementing IPsec with Security Module

This architecture is implemented using Encryption adaptive board with specific encryption chip, which is in the primary place in providing security protection. When system is powered on, Command line interface begins to add Security Policy (SP) to

IPsec engine. Then IPsec engine adds this SP to Forwarding module via Inner Ethernet and this SP is stored in the content-addressable memory (CAM) of Forwarding module. In the condition of manual key configuration, security association (SA) is also added to IPsec engine by Command line interface and then transferred to Security module. SA is a set of policy and keys used to protect traffic. It is stored in the CAM and static random access memory (SRAM) of Security module. Fig. 3 shows the security architecture and Fig. 4 shows the flow chart.

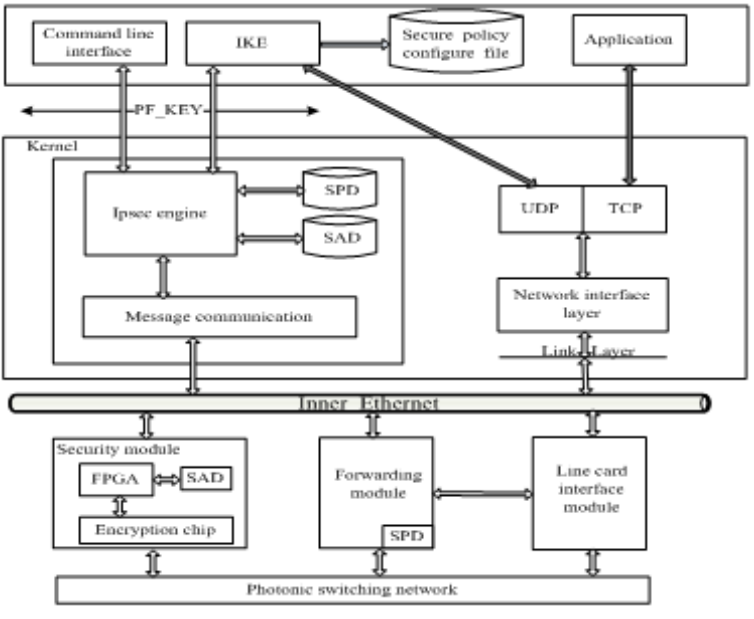

Fig. 3. Secure Architecture of Implementing IPsec with Security Module

For packet passing through the router, it is received by Line card interface module. Packet whose destination is not local router is transferred to Forwarding module. When receiving the packet, Forwarding module executes lookup in its security policy database (SPD) to see whether there has SP for this packet. If it has, the packet will be labeled encryption or decryption tag and forwarded to Security module. Receiving the packet, Security module looks up its security association database (SAD) for SA. If Command line interface didn't add SA manually or this is the first packet of an application, there wouldn't be any SA. In this case, Security module disposes the packet and asks IPsec engine to waken Internet Key Exchange (IKE) for negotiating SA. A major function of IKE is the establishment and maintenance of SAs. The process of IKE for negotiating SA is according to [2]. Otherwise Field Programmable Gate Array (FPGA) performs packet disassembly and controls encryption chip for encryption or decryption. For packet needs encryption, FPGA gets encryption type and encryption key from SAD according to source and destination addresses and protocol type to control Encryption chip for encryption. After encryption, the packet is assembled with packet header by FPGA to construct IPsec packet and the IPsec

packet is sent out through Photonic switching network and Line card interface module. For packet needs decryption, FPGA gets decryption type and decryption key from SAD according to source and destination addresses, protocol type, and security parameter index (SPI), and then control Encryption chip for decryption. After decryption, the packet is assembled again with packet header to construct the original IP packet. Then the decrypted IP packet is also sent out through Photonic switching network and Line card interface module.

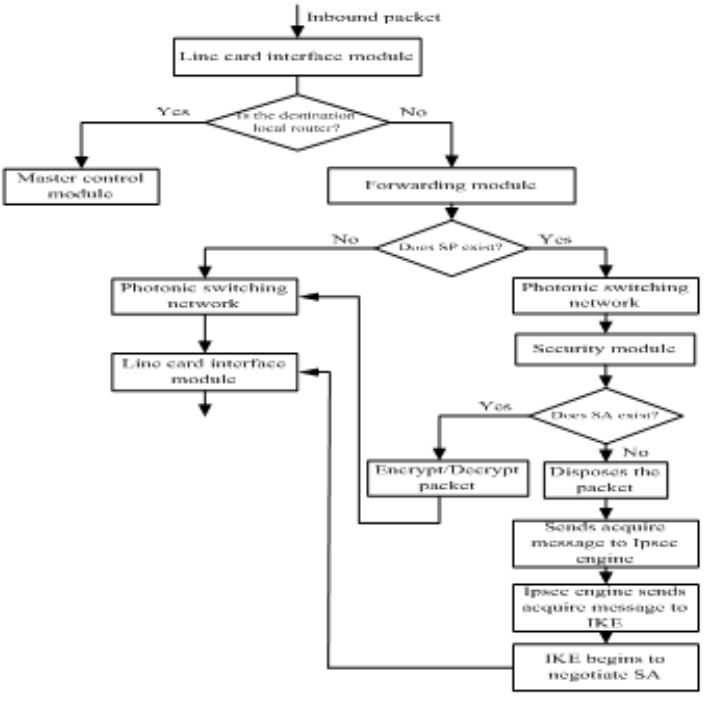

Fig. 4. Flow chart of processing packet with Security module

3.2 Security Architecture of Implementing IPsec Inside Master Control Module

Implementing IPsec inside kernel of Master control module is to deal with the case that data passing through slow path need encryption or decryption, such as the source or the destination address of data is local router. Because these data are almost control messages and are non-real time tasks, they can be encrypted or decrypted inside kernel of Master control module, which is relatively slower. Fig. 5 shows the security architecture.

Flow chart of processing inbound packet is shown in Fig. 6. For inbound packet whose destination is local, it is transferred to IPsec interface of Master control module by Line card interface module. When receiving packet, IPsec interface checks the next header of the packet. If the next header is Authentication Header (AH) or Encapsulating Security Payload (ESP), the packet will be delivered to IPsec inbound processing module. Then IPsec inbound processing module communicates with IPsec

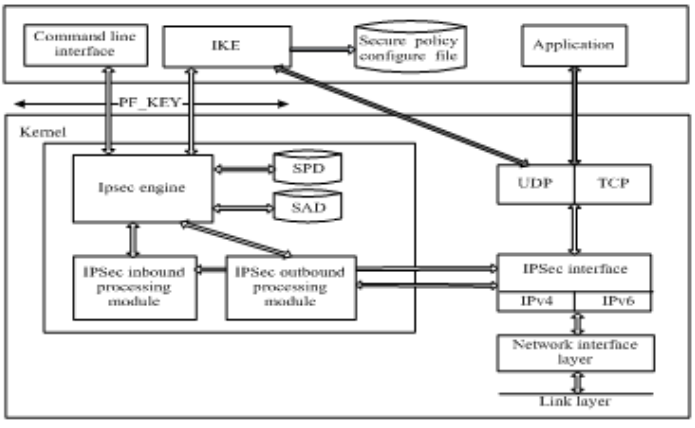

Fig. 5. Security Architecture of Implementing IPsec in Master Control Module

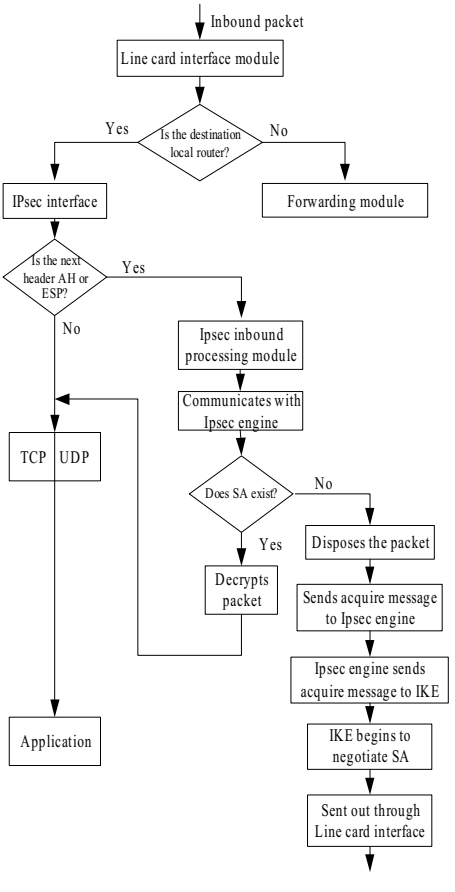

Fig. 6. Flow chart of processing inbound packet with Master Control Module

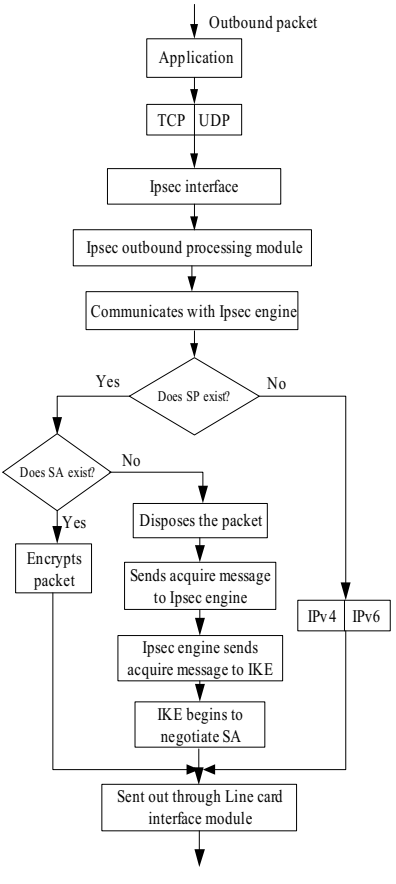

Fig. 7. Flow chart of processing outbound packet with Master control module

engine to get SA and to perform decryption. If SA for this packet does not exist, the packet will be disposed and IPsec engine will send acquire message through PF_KEY socket to IKE to waken IKE for negotiating SA. The Inbound packets destined to the local router but without an AH or ESP header are checked by the other parts of the Master control module, which is not the task of IPsec inside Master control module.

Flow chart of processing outbound packet is shown in Fig. 7. For outbound packets, the packet is first delivered to IPsec outbound processing module to check whether the packet needs encryption. When receiving packet, IPsec outbound processing module communicates with IPsec engine to see whether there has SP for this packet. If it has, IPsec outbound processing module communicates with IPsec engine again for SA to perform encryption. If this SA does not exist, the packet is disposed and IPsec engine asks IKE to negotiate SA. If SP does not exist, the packet is sent back and processed in routine flow. Otherwise the packet is encrypted and sent out through Line card interface module.

4 Testing Architecture

Because security module is processing data passing through the router and IPsec module inside Master control module is processing data that the source or destination is router, we designed two main modes to test both schemes. One mode is using one router, manual SP, and manual SA, and the other is using two routers, manual SP, and automatic SA.

4.1 Test of Security Module with One Router

This mode is used to test correctness of encryption and decryption of Security module with one router and two computers. Testing architecture is shown in Fig. 8. Two computers, acted as Client and Server, were connected to two of Gigabit Ethernet interfaces of SR1880s router, respectively. Data sent from Client to server are encrypted by Security module of the router when passing through SR1880s, and data sent from Server to Client are decrypted by Security module of the router. Manual SP and manual SA are used in this test.

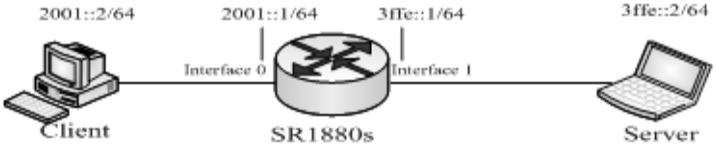

Fig. 8. Architecture of Testing Security Module with One Router

At the beginning of the test, SP and SA were added to Forwarding module and Security module by Command line interface, respectively. To validate correctness of encryption, client ran program which sends raw IPv6 packet. Packet client sent was first received by interface 0 of Line card interface module, was transferred to Forwarding module, and then was forwarded to Security module for encryption. After encryption, the packet was sent out through interface 1 and was finally received by

server. File Client sent was stored in server in advance, so we encrypted the file in server and compared it with received cipher text.

The way to validate correctness of decryption had the similar flow as above. Server encrypted the file and sent it to Client with raw IPv6 packet. The encrypted packet was received by interface 1 of Line card interface module and was forwarded to Security module for decryption. Then the decrypted packet was sent out through interface 0. The packet received by client was in the form of plain text and was compared with the original file saved in advance.

We verified the correctness of encryption and decryption of Security module through testing architecture listed above.

4.2 Test of Security Module with Two Routers

This mode is designed to test the whole IPsec system, including IPsec engine, IKE, and Security module. Testing architecture, with two routers and two computers, is shown in Fig. 9. Two SR1880s were connected with Gigabit Ethernet interfaces and two computers were connected to one of Gigabit Ethernet interfaces of two SR1880s routers, respectively. SP was added to Forwarding module at the beginning of the test. The first packet passing the router would waken IKE to negotiate SA and this SA would be transferred to Security module. We have two methods to validate Security module. The first is using raw IPv6 socket program and the second is using ping.

Fig. 9. Architecture of Testing Security Module with Two Routers

For the first method, Client sent the file using raw IPv6 socket program and server ran the reception program. The first packet wakened IKE to negotiate SA and was disposed by Security module of SR1880s 1. The rest packets were first encrypted by SR1880s 1, then were decrypted by SR1880s 2, and finally were received by server, where we stored the original file in advance to have comparison, in the form of plain text.

For the second method, Client pings server, Internet Control Message Protocol (ICMP) request packet sent by Client was encrypted by Security module of SR1880s 1, and then was decrypted by Security module of SR1880s 2. When server received the ICMP request packet, it sent the ICMP echo packet as reply. The reply packet was first encrypted by Security module of SR1880s 2, then was decrypted by Security module of SR1880s 1, and was finally accepted by client.

We tested the whole IPsec system using two methods listed above with the security architecture shown in Fig. 9. The whole system worked well together.

4.3 Test of IPsec Module Inside Master Control Module with One Router

Implementing IPsec inside Master control module is to process the data that the source or the destination address is local router. To test this module, architecture

shown in Fig. 10 was adopted. Client was connected to one of Gigabit Ethernet interfaces of SR1880s, while server connected to SR1880s using telnet to manipulate the operation in the router. Manual SP and manual SA are also used in this mode. Packet sent from Client to SR1880s was decrypted in Master control module and packet sent from SR1880s to Client was encrypted in Master control module. Encrypted packet Client sent was first received by interface 0 of Line card interface module, and then was transferred to Master control module since the destination address is local. Then the packet was decrypted by IPsec inbound processing module in kernel and was received by reception program ran in application layer. Plain text Client sent was also stored in SR1880s in advance, so we compared the original file with received packet to check the correctness of decryption. Packet SR1880s 1 sent was first encrypted by IPsec outbound processing module in kernel, and then was sent out by Line card interface module through interface 0. Packet, in the form of cipher text, was finally received by Client to check the correctness of encryption.

Fig. 10. Architecture of testing IPsec inside Kernel with One Router

We verified correctness of encryption and decryption of IPsec module inside Master control module through this test. Due to perform encryption and decryption with software, the speed of processing is relatively slower.

4.4 Test of IPsec Module Inside Master Control Module with Two Routers

We also used two methods similar with Fig. 9 to test the whole IPsec module, including IKE, IPsec engine, IPsec inbound processing module, and IPsec outbound processing module. Test architecture is shown in Fig. 11. Client and server were connected to two routers respectively using telnet to manipulate the operation in the routers. Manual SP was added to SPD of IPsec engine in advance. The first packet SR1880s 1 sent would waken IKE to negotiate SA.

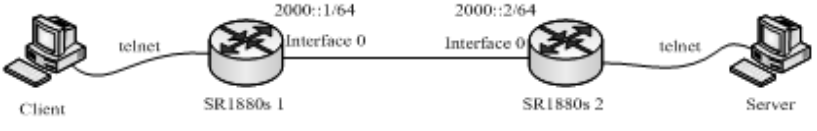

Fig. 11. Architecture of Testing IPsec inside Kernel with Two Routers

For the first method, we ran send program in SR1880s 1 and reception program in SR1880s 2. Packet sent by SR1880s 1 was encrypted by IPsec outbound processing module in kernel of Master control module, and then was sent out through interface 0 of Line card interface module. When interface 0 of SR1880s 2 received the encrypted packet, Line card interface module sent it to Master control module. Then Master control module called IPsec inbound processing module to execute decryption. After

decryption, the packet was finally accepted by reception program ran in SR1880s 2, where stored the original file for checking.

The second method using ping method had the similar flow as in Fig. 9. Internet Control Message Protocol (ICMP) request packet sent by SR1880s 1 was encrypted by IPsec outbound processing module of SR1880s 1, and then was decrypted by IPsec inbound processing module of SR1880s 2. When SR1880s 2 received the ICMP request packet, it sent the ICMP echo packet as reply. The reply packet was first encrypted by IPsec outbound processing module of SR1880s 2, then was decrypted by IPsec inbound processing module of SR1880s 1, and was finally accepted by SR1880s 1.

We also tested the whole IPsec module using two methods above. Testing results show that the whole IPsec module works well together.

5 Conclusion

We presented security architecture which uses two schemes to implement IPsec and adopted it in SR1880s router. One scheme is implementing IPsec with hardware, which processing the data passing through fast path; the other is implementing IPsec inside kernel of Master control module of the router with software to process the data passing through slow path. Two schemes working together will process data in time with encryption chip and will also protect non-real time tasks in slow path. Testing results show that two schemes work well together and protect the traffic passing through the router.

Problem we still facing is the mismatch of processing speed between Security module, known as 2.5Gbps to 10Gbps, and Forwarding module, usually known as 10Gbps up to 40Gbps. How to improve the processing speed of Security module while not sacrificing the security is the next work we will research.

References

1. S. Kent and R. Atkinson “Security Architecture for the Internet Protocol”, IETF RFC 2401, November 1998.
2. D**.** Harkins and D. Carrel, “The Internet Key Exchange (IKE)”, IETF RFC 2409, November 1998.
3. Charlie Kaufman, “Internet Key Exchange (IKEv2) Protocol”, IETF RFC 4306, Deembler 2005.
4. Ximing Hu, Jing Qu, Binqiang Wang, Xiaobei Li, “CISOQ: A Practical High-Performance Packet Switch Architecture for the Support of Multicast Traffic”, in *2005 Proc. PDCAT Conf.*, Dalian, China, pp. 139-143
5. Chen Yue, Dong Yuguo, Lin Yusong, Lan Julong. “A Packet-Order-Keeping-Demultiplexer in Parallel-Structure Router Based on Flow Classification”, in *2003 Proc. ICCNMC Conf.* Shanghai, China, pp.
6. Li Yufeng, Yi Peng, Qiu Han, Lan Julong, “Sizing buffers for pipelined forwarding engine”, in *2006 Proc. ICCCAS Conf.,Guilin, China,* accepted.
7. Cássio Ditzel Kropiwiec, Edgard Jamhour, Carlos Maziero, “A Architecture for Protecting Web Sevices with IPsec”, in *2004 Proc. EUROMICRO Conf.*, Rennes, France, pp. 290-297
8. Jonathon Trostle and Bill Gossman. “Techniques for improving the security and manageability of IPsec policy”. *International Journal of Information Security*, vol. 4, no. 3, pp. 209–226, Jun. 2005.