10 Giga급 VPN 가속보드 설계 및 구현

김기현* · 한종욱*
*한국전자통신연구원

Design and Implementation of 10 Giga VPN Acceleration Board

Ki Hyun Kim* · Jong Uk Han*
*Electronics and Telecommunications Research Institute
E-mail : kihyun@etri.re.kr, hanjw@etri.re.kr

요 약

최근 네트워크 환경에서 보안과 속도는 항상 trade-off가 존재한다. 최근에 개발된 보안 프로세서들은 성능이 매우 향상되고, 많은 부분의 보안 관련 알고리즘이 하드웨어로 구현되어 있다. 이런 고속 보안 프로세서는 매우 큰 대역폭을 요구하는 현 네트워크 보안 솔루션 장비 개발에는 필수 요소가 된다. 본 논문에서는 10 Giga급 VPN 장비의 설계 및 구현에 대해서 기술하고자 한다. 본 시스템에서는 Cavium사의 Nitrox-II 프로세서를 사용하여 10 Giga를 구현하였고, 두개의 SPI-4.2 인터페이스와 PCI 인터페이스를 지원한다. 지원하는 암호 알고리즘은 상용 VPN 장비와의 호환성을 위하여 상용 VPN 장비에서 사용되는 암호 알고리즘은 모두 지원되며 및 국내에서 개발된 SEED 알고리즘도 지원한다. IPsec 및 SSL 프로토콜을 지원하고, 고속 처리에 유리한 In-Line 구조 및 NPU(Network Processor Unit)의 활용도에 유리한 Look-Aside 구조 모두를 지원하도록 설계 하였다.

ABSTRACT

Trade-off of security and speed always exists in the latest network environment. Recently, developed security processors is improved very performance, and security connection algorithms of a lot of part were embodied by hardware. This high speed security processor is essential ingredient in string network security solution equipment development that require very big band width. In this paper, we wish to describe about design and implementation of 10 Giga VPN equipments. In this system, embodied 10 Giga to use Cavium company's Nitrox-II processor, and supports two SPI4-2 interface and PCI interface. All of the password algorithm that password algorithm that support is used in common use VPN equipment for compatibility with common use VPN equipment are supported and support SEED algorithm developed in domestic. Designed to support IPsec and SSL protocol, and supports all of In-Line structure that is profitable in high speed transaction and the Look-Aside structure that is profitable in practical use degree of NPU(Network Processor Unit).

키워드
보안프로세서, 가상사설네트워크

Ⅰ. 서 론

최근 급증하고 있는 온라인 거래와 다양한 인터넷 서비스의 확대로 인하여 많은 사람들이 쉽게 정보를 주고받거나, 얻을 수 있다. 그러나 바이러스 또는 해킹과 같은 사이버 테러로 인하여 개인의 사생활 정보 유출은 물론 국가적 안보까지 위협하고 있다. 이러한 네트워크 환경에서 정보를 보호하기 위한, 가상사설망(VPN : Virtual Private Network), 방화벽(Firewall), 침입탐지(IDS : Intrusion Detection System) 등과 같은 정보 보호 기술과 제품들이 다양하게 개발 되고 있다. 최근에는 2개 이상의 기능이 통합된 장비들이 출시되고 있다.

이들 정보 보호 관련 기술 중 VPN 기술은 네트워크 망을 효율적으로 사용하기 위한 네트워크 기술이면서 동시에 네트워크 정보 보안을 위한 정보

보호 기술이다. 따라서 VPN 보안 장비는 이러한 두 가지 측면을 고려하여 설계되어야 한다. 무엇보다 VPN의 보안 기능을 가능하게 해주는 기술은 크게 터널링 기술과 암호화 기술이 있다. 터널링 프로토콜로는 PPTP, L2TP, IPsec 등이 있다. 이중 IPsec은 가장 강력하고 융통성을 제공하는 터널링 프로토콜이며, VPN 보안 장비는 이를 기본적으로 지원해야 한다. 또한 고속 VPN 보안 장비에서 암호화 기능을 구현하기 위해서는 고속의 암호/복호 기능이 필요하며, 이를 구현하기 위해서는 고속 보안 프로세서의 사용이 필수적이다. [1]~[3]

본 논문에서는 라우터, 게이트웨이, 그리고 망 관련 시스템에 사용될 수 있는 VPN 가속모듈을 제안한다. VPN 가속모듈은 10 Giga급 보안 프로세서를 이용한 간략한 VPN 가속보드 형태로 구현하였다.[5]

본 논문의 2장에서는 VPN 가속보드의 개요 및 전체적인 구성에 대해서 설명하고, 3장에서는 각 유닛별 세부 기능 및 동작 흐름을 상세하게 기술하고, 마지막 4장에서는 결론을 기술하였다.

II. VPN 가속보드

1. VPN 가속보드의 개요

VPN 가속보드는 네트워크 환경에서 게이트웨이, 라우터, 네트워크 관리 시스템, 또는 단말기 상호간의데이터 및 제어 정보 등을 보호하기 위하여 IPsec 등을 기반으로 안전한 채널을 구축하고, 또한 시스템간의 사용자 트래픽에 대한 VPN 서비스를 제공하는 것을 목적으로 제작하는 하드웨어 보드이다.[6]

2. 제공 기능

VPN 가속보드가 제공하는 기본적인 기능과 그 성능은 다음과 같다.

- IPsec 기능 제공 :
  IPsec 핵심기능을 최대한 H/W화함으로써 10Gbps의 IPsec 처리를 지원한다. (1터널, 3-DES 사용 시) 이러한 성능을 제공하기 위해서 본 논문에서는 Cavium사의 Nitrox-II 보안 프로세서를 사용하였다. 또한 VPN 서비스 제공 및 신뢰채널 형성 시 기존 게이트웨이, 라우터, 네트워크 관리 시스템의 성능저하가 최소화되도록 In-line 구조를 지원하고, 필요에 따라 게이트웨이, 라우터, 네트워크 관리 시스템에서 암/복호화 기능만의 사용이나 SSL 프로토콜의 사용이 용이하도록 Look-Aside구조를 지원한다.
- 다양한 네트워크 및 버스 인터페이스 제공 :
  VPN 가속보드는 고속으로 데이터를 효율적으로 처리하기 위해서 상용 MAC 칩과 Network Processor Unit(NPU)에서 사용되고 있는 데이터 인터페이스를 제공한다.
- PIC/PIC-X 인터페이스 : 32/64 bits, 33/66/133 MHz. Host / Control Processor
- SPI4-2 인터페이스 : OC192 Framer / MAC or NPU
- 다양한 알고리즘 제공 :
  VPN 가속보드에서 제공되는 암호 알고리즘은 상용 보안시스템에서 많이 사용되는 암호 알고리즘들 중심으로 제공한다. 또한 국내 표준 암호 알고리즘인 SEED가 제공 된다. 지원하는 암호 알고리즘은 다음과 같다.
- 암호 알고리즘 : 3DES/ DES, AES, RC4, RSA, SEED
- 인증
  MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- 다양한 보안 프로토콜 지원 :
  VPN 가속보드는 기본적으로 IPsec 보안 프로토콜을 이용한 VPN 서비스를 제공한다. 또한 필요에 따라 SSL도 지원한다.

3. 전체 구조 및 구성

VPN 가속보드는 크게 보안프로세서, SEED 구현 FPGA, 그리고 SPI4-2 및 PCI 외부 인터페이스 부분으로 구성된다. 암호프로세서는 Cavium사의 Nitrox-II 보안 프로세서로써 두개의 SPI4-2 포트와 PCI/PCI-X 인터페이스를 제공하여 10Gbps 이상의 고속 데이터 처리가 가능하다. 국내에서 개발된 SEED 암호 알고리즘은 한 개의 FPGA칩으로 구현하였고, 제어 프로세서 및 보안프로세서와는 64bit 66MHz의 PCI 인터페이스로 데이터 입출력 및 제어가 이루어진다.[4][7] VPN 가속보드의 전체 구성 블록도는 그림 1과 같다.

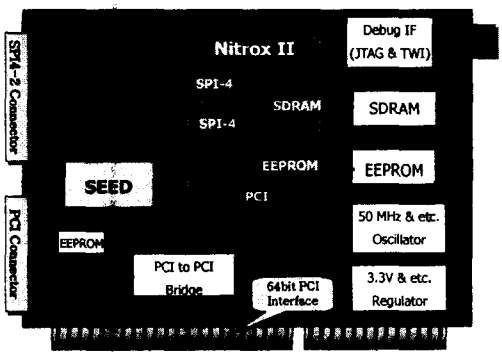

그림 1. VPN 가속보드 전체 블록도

III. 유닛별 세부 설계

1. 보안프로세서 유닛

본 절에서는 보안프로세서 유닛에 대해서 기술하며, 그 중에서도 본 유닛의 가장 핵심인 보안프

로세서를 상세하게 설명하고자 한다. 보안프로세서 유닛은 여러 평가에 방법에 의해 선정된 Nitrox-II 보안프로세서를 중심으로 구현하였다.

보안프로세서 유닛에 사용된 Nitrox-II 보안프로세서는 2003년 Cavium사에서 제작한 것으로, 고속의 암호 처리 능력을 가지고 있으며, 다양한 프로토콜을 지원하는 암호처리 단일 칩이다. 이는 고속의 산술연산 모듈과 랜덤 수 생성기, 해쉬 처리 모듈이 하드웨어로 구현되어 가능하다. 또한 SSL/TLS 또는 IPsec/IKE 암호 프로토콜을 지원한다. Nitrox-II 프로세서는 내부 코어가 Giga급 처리가 가능하도록 설계되어 있으며, 여러 암호 연산이 병렬로 처리 가능하도록 설계되어 있어 더욱 고속처리와 시스템 설계 용통성을 제공한다.

본 보안프로세서 유닛에서 사용한 Nitrox-II 보안프로세서의 기능 및 성능 다음과 같다.[4]

- 단일 칩으로 SSL/TLS, IPsec/IKE와 같은 암/복호 프로토콜을 고속으로 지원
- 기능적으로 In-Line 데이터 처리가 가능하여 Bump-in-the-wire 장비를 구현할 수 있고, 주변의 NPU와 Framer/MAC 등 장비와의 다양한 호환성을 제공
- L2 & L3 Parsing이 가능
- Inbound 시 SA Lookup 기능 제공
- 다양한 알고리즘 지원
  - ✓ RSA와 Diffie-Hellman
  - ✓ DES/3DES, AES, ARC4
  - ✓ MD5, SHA-1, HMAC-MD5, HMAC-SHA-1
- 고속의 프로토콜 구현
  - ✓ 최대 40,000 SSL TPS
  - ✓ 최대 10,000 IKE Main Mode/sec (DH (1024bit) + RSA의 동작 속도를 의미 함)
- 많은 수의 IPsec SA 또는 SSL Contexts 지원
  - ✓ 2M IPsec SAs, 512MB DDR-SDRAM 환경
  - ✓ 4M SSL Contexts, 4GB DDR-SDRAM 환경
- 고속 데이터 암호화
  - ✓ IPsec 응용분야 : 5G ~ 20Gbps
  - ✓ SSL 응용분야 : 최대 20Gbps
- 최대 320 Mbps Random Number Generator
- 고속의 표준 인터페이스
  - ✓ PCI/PCI-X ; 32/64-bit, 33/66/133 MHz
  - ✓ SPI4-2
- FIPS 140-2 Level 3-4 지원

Linux, BSD, Windows, VxWorks를 위한 S/W 드라이버 지원

2. SEED 유닛

본 절에서는 SEED 암호 유닛에 대해서 기술한다. 본 SEED 암호 유닛은 SEED 암호 알고리즘을 한국전자통신연구원에서 설계한 SEED FPGA와 SEED 프로그램 저장 장치인 두개의 EEPROM으로 구현하였다. 사용된 FPGA 칩은 Xilinx VectexII-Pro XC2VP7이며, EEPROM은 4Mbyte의 XC18V04 소자를 이용하였다.

가. 개요

SEED암호 알고리즘은 Fiestel 구조로 이루어져 있으며, 128bit 입력 데이터와 키를 이용하여 16round의 연산을 수행하여128bit의 출력 데이터를 생성한다. SEED 암호 연산을 위한 각 round마다 64bit의 round key를 사용하며, 이때 각 round마다 필요한 round key는 초기 입력되는 128bit의 키로부터 유도되어 진다. 그림 2에 SEED 암호 알고리즘의 전체 구조를 나타내었다.[7]

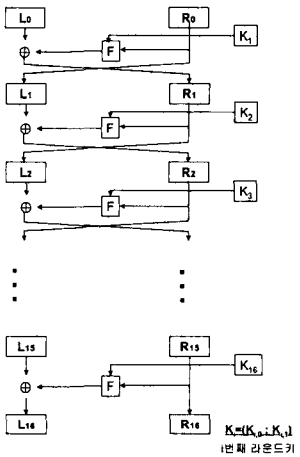

그림 2 SEED 알고리즘 구조

나. F-함수

SEED 암호 알고리즘의 F-함수는 64bit의 데이터와 64bit의 round key를 입력으로 받아서 64bit의 데이터를 출력한다. 다른 대칭키 암호 알고리즘에 비해 SEED의 성능이 느린 것은 바로 F-함수의 영향인데, 연산을 수행하는 과정에서 32bit의 블록으로 덧셈 연산이 3차례에 걸쳐 serial 연결된다.

다. G-함수

SEED의 G-함수를 수식으로 표현하면 식 1과 같다.

$$Y_3 = S_2(X_3),\ Y_2 = S_1(X_2),\ Y_1 = S_2(X_1),\ Y_0 = S_1(X_0),$$

$$\begin{aligned} Z_3 &= (Y_0 \& m_3) \oplus (Y_1 \& m_0) \oplus (Y_2 \& m_1) \oplus (Y_3 \& m_2) \\ Z_2 &= (Y_0 \& m_2) \oplus (Y_1 \& m_3) \oplus (Y_2 \& m_0) \oplus (Y_3 \& m_1) \\ Z_1 &= (Y_0 \& m_1) \oplus (Y_1 \& m_2) \oplus (Y_2 \& m_3) \oplus (Y_3 \& m_0) \\ Z_0 &= (Y_0 \& m_0) \oplus (Y_1 \& m_1) \oplus (Y_2 \& m_2) \oplus (Y_3 \& m_3) \end{aligned}$$

$$(m_0 = 0\text{xfc},\ m_1 = 0\text{xf3},\ m_2 = 0\text{xcf},\ m_3 = 0\text{x3f})$$

식 1. G-함수의 표현

라. S-Box

SEED의 S-Box는 8bit의 데이터를 입력으로 받아 8bit의 출력을 내는 함수로, S1, S2의 2개의 함수로 구성되며, 식 2.와 같은 4개의 SS-Box들을 정의해서 사용한다.

$$SS_3 = S_2(X_3)\&m_2 \,\|\, S_2(X_3)\&m_1 \,\|\, S_2(X_3)\&m_0 \,\|\, S_2(X_3)\&m_3,$$
$$SS_2 = S_1(X_2)\&m_1 \,\|\, S_1(X_2)\&m_0 \,\|\, S_1(X_2)\&m_3 \,\|\, S_1(X_2)\&m_2,$$
$$SS_1 = S_2(X_1)\&m_0 \,\|\, S_2(X_1)\&m_3 \,\|\, S_2(X_1)\&m_2 \,\|\, S_2(X_1)\&m_1,$$
$$SS_0 = S_1(X_0)\&m_3 \,\|\, S_1(X_0)\&m_2 \,\|\, S_1(X_0)\&m_1 \,\|\, S_1(X_0)\&m_0,$$

(여기서, || 는 concatenation).

$$Z = SS_3(X_3) \oplus SS_2(X_2) \oplus SS_1(X_1) \oplus SS_0(X_0)$$

식 2. SS-Box를 이용한 G-함수의 구현

그러나 이러한 SS-Box의 사용은 그냥 S1, S2-Box를 사용하는 경우보다 Memory 공간을 더욱 많이 사용(16배 : 4K byte)하므로 Hardware 구현의 측면에서는 비효율적으로 보인다.

마. Round Key 생성

SEED 암호 연산을 수행하기 위해 사용되는 라운드 키는 먼저, 128bit 키를 64bit씩 나눈 후, 이 값들을 교대로 8bit씩 좌, 우로 회전 이동하고, 32bit씩 간단한 산술 연산(덧셈과 뺄셈)과 G-함수를 적용하여 생성한다.

3. 외부 인터페이스 유닛

본 절에서는 VPN 가속보드의 SPI4-2 및 PCI 등 외부 인터페이스에 대해서 기술하고자 한다. Nitrox-II에서 제공되는 SPI4-2 인터페이스는 최소 311MHz에서 최대 500MHz를 지원하여, 최소 9.7Gbps에서 최대 15.6Gbps까지의 데이터 전송율을 지원한다. [14]

VPN 가속보드에서 PCI 인터페이스는 SEED FPGA칩과의 인터페이스를 위하여 전체적으로 64bit, 66MHz를 지원하도록 설계하였다. 또한 개발 환경 및 VPN 가속보드의 활용에 따라 제어신호와 패킷 데이터를 처리하는 것이 용이하게 하기 위해서 PCI Connector와 PCI 슬롯 인터페이스 모두를 지원하도록 설계하였다.[8]

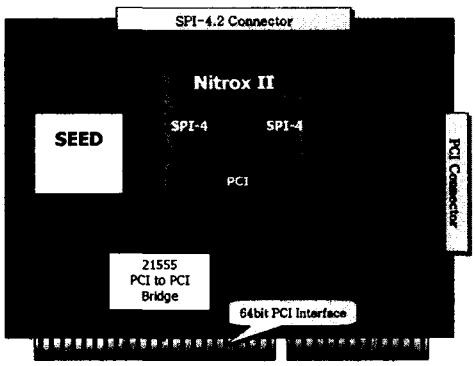

그림 3. VPN 가속보드의 외부 인터페이스

IV. 결 론

최근에 개발된 보안 프로세서들은 성능이 매우 향상되고, 많은 부분의 보안 관련 알고리즘이 하드웨어로 구현되어 있다. 이런 고속 보안 프로세서는 매우 큰 대역폭을 요구하는 현 네트워크 보안 솔루션 장비 개발에는 필수 요소가 된다. 본 논문에서는 10 Giga급 VPN 가속보드 설계에 대해서 기술하였다. 본 시스템은 상용 VPN 장비와의 호환성을 위하여 상용 VPN 장비에서 사용되는 암호 알고리즘은 모두 지원하며, 국내에서 개발된 SEED 알고리즘도 지원한다. 또한 두개의 SPI-4.2 인터페이스와 PCI 인터페이스를 지원하여 고속 처리에 유리한 In-Line 구조 및 NPU(Network Processor Unit)의 활용도에 유리한 Look-Aside 구조 모두를 지원하도록 설계 하였다.

현재 한국전자통신연구원에서 설계된 VPN 가속보드는 PCB 설계 과정과 PCB 시뮬레이션 과정을 마치고, PCB 제작 완료되었다.

참고 문헌

[1] 주학수, 주홍돈, 김승주, "고속 암호연산 프로세서 개발현황", 정보보호학회지, 제12권 3호, 2002

[2] Neil Gammage, "Security Application Note", Motorola Canada, 2001

[3] 이계상, "IPsec 표준화 동향", KISA동향특집, 2000. 8

[4] "NITROX-II Security Processor CN25xx Family Hardware Manual Rev0.1", Cavium, 2003. 6.

[5] "CN-EB2200 Schematic Rev AX01", Cavium, 2003. 5

[6] "CN-EB2500 Schematic Rev AX01", Cavium, 2003. 2.

[7] "차세대 암호알고리듬 동향", 류희수, 정교일, 한국전자통신연구원/주간기술동향, 1052호, 2002. 6.

[8] "System Packet Interface Level 4(SPI-4) Phase 2: OC-192 System Interface for Physical and Link Layer Devices", 2001. 1.