(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0107978
(43) 공개일자 2019년09월23일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) *G06F 9/54* (2018.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 69/18 (2013.01)
G06F 9/54 (2013.01)
(21) 출원번호 10-2018-0029363
(22) 출원일자 2018년03월13일
심사청구일자 2018년03월13일

(71) 출원인
(주) 시스메이트
대전광역시 유성구 유성대로1184번길 41(신성동)
(72) 발명자
서규호
세종특별자치시 남세종로 358, 208동 1702호(소담동, 새샘마을2단지)
최간호
대전광역시 서구 관저중로 33, 110동 102호(관저동, 관저예미지 명가의 풍경)
유인규
경기도 수원시 영통구 영통로 498, 138동 1804호(영통동, 황골마을주공1단지아파트)
(74) 대리인
특허법인 신지

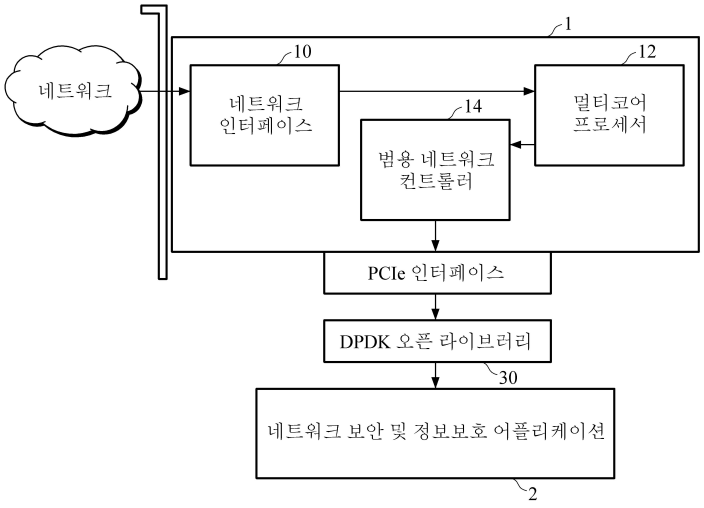
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 **멀티 코어 프로세서 및 범용 네트워크 컨트롤러 하이브리드 구조의 네트워크 인터페이스 카드**

(57) 요 약

멀티 코어 프로세서 및 범용 네트워크 컨트롤러 하이브리드 구조의 네트워크 인터페이스 카드가 개시된다. 일 실시 예에 따른 네트워크 인터페이스 카드는, 네트워크를 통한 패킷 송수신을 위한 네트워크 인터페이스와, 네트워크 보안 및 정보보호 기능을 가속화하는 멀티 코어 프로세서와, 다수의 운영체제 및 시스템에 대한 호환성을 제공하여 멀티 코어 프로세서를 위한 별도의 디바이스 드라이버가 필요 없는 범용 네트워크 컨트롤러를 포함한다.

대 표 도



(52) CPC특허분류
H04L 63/166 (2013.01)
H04L 67/2861 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 S2496941
부처명 중소기업청
연구관리전문기관 중소기업기술정보진흥원
연구사업명 혁신형기술개발사업
연구과제명 고성능 보안 가속 프로세서를 내장한 네트워크 인터페이스 카드 개발
기 여 율 1/1
주관기관 ㈜시스메이트
연구기간 2017.06.19 ~ 2019.06.18

명 세 서

청구범위

청구항 1

네트워크를 통한 패킷 송수신을 위한 네트워크 인터페이스;

네트워크 보안 및 정보보호 기능을 가속화하는 멀티 코어 프로세서; 및

다수의 운영체제 및 시스템에 대한 호환성을 제공하여 상기 멀티 코어 프로세서를 위한 별도의 디바이스 드라이버가 필요 없는 범용 네트워크 컨트롤러;

를 포함하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 2

제 1 항에 있어서, 상기 네트워크 인터페이스는

10Gbps 이더넷 4 포트를 지원하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 3

제 1 항에 있어서, 상기 멀티 코어 프로세서는

트래픽의 암복호화 기능을 가속화하는 암복호화 가속기;

패턴 매칭 기능을 가속화하는 패턴 매칭 가속기; 및

보안 필터 기능을 가속화하는 보안 필터 가속기;

를 포함하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 4

제 1 항에 있어서, 상기 범용 네트워크 컨트롤러는

네트워크 가상화 기능을 제공하여 멀티 코어 프로세서의 부하를 절감하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 5

제 4 항에 있어서, 상기 범용 네트워크 컨트롤러는

단일 루트 입출력 가상화(Single Root I/O Virtualization: SR-IOV) 기반의 네트워크 가상화 가속 기능을 제공하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 6

제 1 항에 있어서, 상기 범용 네트워크 컨트롤러는

데이터 플레인 개발 키트(Data Plane Development Kit: DPDK, 이하 'DPDK'라 칭함) 기반 고속 병렬 패킷 처리 가속 기능을 제공하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 7

제 1 항에 있어서, 상기 범용 네트워크 컨트롤러는

DPDK 공개 소프트웨어를 통해, 서버 기반 네트워크 보안 및 정보보호 어플리케이션이 커널을 통과하여 직접 네트워크 인터페이스 카드에 액세스할 수 있도록 하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 8

제 1 항에 있어서, 상기 범용 네트워크 컨트롤러는

클라우드 가상 서버의 네트워크 인터페이스의 가상 오픈 스위치(Open vSwitch: OvS) 가속 기능을 지원하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 9

제 1 항에 있어서, 상기 네트워크 인터페이스 카드는

상기 멀티 코어 프로세서에 보안 가속 기능을 오프로드하여 네트워크를 통해 송수신되는 트래픽을 대상으로 트래픽 암복호화 및 패턴 매칭을 포함한 전처리를 수행하고,

상기 멀티 코어 프로세서를 통한 전처리 이후, 상기 범용 네트워크 컨트롤러를 이용하여 DPDK 최적화를 포함한 트래픽 후처리를 수행하며 DPDK 공개 소프트웨어를 통해 고속 패킷 처리를 오프로드하여 네트워크 보안 및 정보보호 어플리케이션과 트래픽을 송수신하는 것을 특징으로 하는 네트워크 인터페이스 카드.

청구항 10

네트워크 보안 및 정보보호 기능을 가속화하는 멀티 코어 프로세서와, 다수의 운영체제 및 시스템에 대한 호환성을 제공하여 상기 멀티 코어 프로세서를 위한 별도의 디바이스 드라이버가 필요 없는 범용 네트워크 컨트롤러를 포함하는 하이브리드 구조의 네트워크 인터페이스 카드; 및

상기 네트워크 인터페이스 카드가 장착된 네트워크 보안 및 정보보호 어플리케이션 서버;

를 포함하는 것을 특징으로 하는 네트워크 보안 및 정보보호 어플라이언스 시스템.

청구항 11

제 10 항에 있어서, 상기 네트워크 보안 및 정보보호 어플라이언스 서버는

상기 네트워크 인터페이스로부터 입력되는 패킷을 DPDK 공개 소프트웨어를 이용하여 병렬 처리함에 따라 부하를 제거하고, 불균일 메모리 접근(Non-Uniform Memory Access: NUMA)를 이용하여 패킷을 코어 별로 분산 처리하는 것을 특징으로 하는 네트워크 보안 및 정보보호 어플라이언스 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 트래픽 처리 및 관리기술에 관한 것이다.

배 경 기 술

[0002] 최근 ICBM(IoT, Cloud, Big Data, Mobile)의 확대로 모든 사물이 네트워크 연결되고, 광대역 통신 서비스 수요가 급증함에 따라 사이버 보안 산업이 한층 주목 받고 있다. 특히 네트워크 보안, 정보보호 분야에서는 고도화되는 사이버 위협에 대응하기 위해서 대용량의 트래픽을 실시간으로 정밀하게 처리할 수 있는 성능을 요구하고 있다. 아울러 웹 2.0 인터넷 서비스의 확대로 암호화 트래픽이 50% 이상으로 증가하고 있어, 실시간 패킷 처리 성능이 더욱더 문제가 되고 있다. 그러나 대부분의 기업은 다중 CPU 성능에 의존한 서버 시스템을 이용한 어플라이언스(Appliance)를 제작하여 보안 소프트웨어를 공급하고 있어 성능 경쟁력 면에서 경쟁 열위를 면치 못하고 있다.

[0003] 네트워크 인터페이스 카드(Network Interface Card: NIC)는 네트워크 인터페이스 컨트롤러(Network Interface Controller), 네트워크 어댑터(network adapter), 랜 카드, 랜 어댑터(LAN adapter) 등으로 불리는 컴퓨터 하드웨어 구성품으로서, 컴퓨터를 인터넷 또는 사내 망에 연결 시키기 위한 통신 기능을 제공한다. 최근 10기가급 이더넷 기술이 일반화됨에 따라 네트워크 어댑터의 네트워킹 프로토콜은 이더넷 기반으로 통합되고 있다. 침입차단 시스템(Intrusion Prevention System: IPS), 내부 정보 유출 방지(Data Loss Prevention: DLP) 시스템과 같은 네트워크 보안 시스템의 네트워크 장비로서 패킷 처리 성능이 이슈가 되면서 해외 벤더를 중심으로 네트워크 보안 전용 네트워크 인터페이스 카드 제품이 출시되어 왔다.

[0004] 인터넷 서비스의 경우, 데이터 보안을 위해 보안 소켓 계층(Secure Socket Layer: SSL)과 같은 개인정보 유지 프로토콜을 이용하고 있다. 사이버 공격의 상당수가 암호화된 네트워크 트래픽을 주요 공격 경로로 사용하고 있

으며, 현재 보안 시스템은 SSL 트래픽 내부의 위협을 인식하거나 차단하지 못하고 있다. SSL 암복호화 기술은 어플라이언스 단독형으로 개발되어 복호화된 트래픽을 미러링 하여 침입 탐지 시스템(Intrusion Detection System: IDS), 침입 차단 시스템(Intrusion Prevention System: IPS), 내부 정보 유출 방지(Data Loss Prevention: DLP) 시스템, 포렌식(Forensic) 시스템 등의 보안장비들로 전송하는 방식으로 제품이 공급되고 있다. 단독형 어플라이언스 방식의 SSL 암복호화 솔루션은, 설치와 구성의 복잡성이 높고 장애 포인트가 증가한다. 따라서, SSL 암복호화 기술을 통합하는 방식의 솔루션을 개발하기 위해 노력하고 있으나, CPU와 메모리의 사용이 높은 SSL 암복호화 기술로 인해 성능적인 이슈가 발생하여 새로운 솔루션이 필요하다.

발명의 내용

해결하려는 과제

[0005] 일 실시 예에 따라, 네트워크 보안 솔루션의 성능저하 문제를 해결하기 위해 멀티 코어 프로세서 및 범용 네트워크 컨트롤러 하이브리드 구조의 네트워크 인터페이스 카드를 제안한다.

과제의 해결 수단

[0006] 일 실시 예에 따른 네트워크 인터페이스 카드는, 네트워크를 통한 패킷 송수신을 위한 네트워크 인터페이스와, 네트워크 보안 및 정보보호 기능을 가속화하는 멀티 코어 프로세서와, 다수의 운영체제 및 시스템에 대한 호환성을 제공하여 멀티 코어 프로세서를 위한 별도의 디바이스 드라이버가 필요 없는 범용 네트워크 컨트롤러를 포함한다.

[0007] 네트워크 인터페이스는, 10Gbps 이더넷 4 포트를 지원할 수 있다.

[0008] 멀티 코어 프로세서는, 트래픽의 암복호화 기능을 가속화하는 암복호화 가속기와, 패턴 매칭 기능을 가속화하는 패턴 매칭 가속기와, 보안 필터 기능을 가속화하는 보안 필터 가속기를 포함할 수 있다.

[0009] 범용 네트워크 컨트롤러는, 네트워크 가상화 기능을 제공하여 멀티 코어 프로세서의 부하를 절감할 수 있다. 이때, 범용 네트워크 컨트롤러는 단일 루트 입출력 가상화(Single Root I/O Virtualization: SR-IOV) 기반의 네트워크 가상화 가속 기능을 제공할 수 있다.

[0010] 범용 네트워크 컨트롤러는, 데이터 플레인 개발 키트(Data Plane Development Kit: DPDK, 이하 'DPDK'라 칭함) 기반 고속 병렬 패킷 처리 가속 기능을 제공할 수 있다. 범용 네트워크 컨트롤러는, DPDK 공개 소프트웨어를 통해, 서버 기반 네트워크 보안 및 정보보호 어플리케이션이 커널을 통과하여 직접 네트워크 인터페이스 카드에 액세스할 수 있도록 할 수 있다. 범용 네트워크 컨트롤러는, 클라우드 가상 서버의 네트워크 인터페이스의 가상 오픈 스위치(Open vSwitch: OvS) 가속 기능을 지원할 수 있다.

[0011] 네트워크 인터페이스 카드는, 멀티 코어 프로세서에 보안 가속 기능을 오프로드하여 네트워크를 통해 송수신되는 트래픽을 대상으로 트래픽 암복호화 및 패턴 매칭을 포함한 전처리를 수행하고, 멀티 코어 프로세서를 통한 전처리 이후, 범용 네트워크 컨트롤러를 이용하여 DPDK 최적화를 포함한 트래픽 후처리를 수행하며 DPDK 공개 소프트웨어를 통해 고속 패킷 처리를 오프로드하여 네트워크 보안 및 정보보호 어플리케이션과 트래픽을 송수신할 수 있다.

[0012] 다른 실시 예에 따른 네트워크 보안 및 정보보호 어플라이언스 시스템은, 네트워크 보안 및 정보보호 기능을 가속화하는 멀티 코어 프로세서와 다수의 운영체제 및 시스템에 대한 호환성을 제공하여 멀티 코어 프로세서를 위한 별도의 디바이스 드라이버가 필요 없는 범용 네트워크 컨트롤러를 포함하는 하이브리드 구조의 네트워크 인터페이스 카드와, 네트워크 인터페이스 카드가 장착된 네트워크 보안 및 정보보호 어플리케이션 서버를 포함한다.

[0013] 네트워크 보안 및 정보보호 어플라이언스 서버는, 네트워크 인터페이스로부터 입력되는 패킷을 DPDK 공개 소프트웨어를 이용하여 병렬 처리함에 따라 부하를 제거하고, 불균일 메모리 접근(Non-Uniform Memory Access: NUMA)를 이용하여 패킷을 코어 별로 분산 처리할 수 있다.

발명의 효과

[0014] 멀티 코어 프로세서 및 범용 네트워크 컨트롤러 하이브리드 구조의 네트워크 인터페이스 카드를 제공함에 따라, 고성능을 요구하는 트래픽 암복호화, 패턴매칭 등과 같은 네트워크 보안 가속 기능을 오프로드(offload)하고,

고속 패킷 병렬 처리 기능을 오프로드 함에 따라, 네트워크 패킷 처리 성능 부하를 줄일 수 있다.

[0015] 본 발명이 적용되는 분야는 다음과 같다. 네트워크 보안 제품 공급자에게, 네트워크 침입 탐지/차단(IDS/IPS) 시스템, 분산 서비스 거부 공격 방어(Anti-DDoS) 시스템, 네트워크 통합 보안(Unified Threat Management: UTM) 시스템, 차세대 방화벽(Next Generation Firewall)의 PCRE 패턴 매칭 가속 NIC 기능을 제공할 수 있다. 네트워크 정보보호 제품 공급자에게, 내부 정보 유출 방지(Data Loss Prevention: DLP) 시스템, 웹 방화벽 시스템, 이메일 필터 시스템, 데이터베이스 보안 시스템 등의 SSL 암복호화 가속 NIC 기능을 제공할 수 있다. 통신 사업자 및 서비스 사업자에게, 대용량 ISP 네트워크의 트래픽 수집·측정·제어·관리 시스템, 플로우 또는 응용 서비스 단위의 QoS 제어 및 관리 시스템, 인터넷 응용 어플리케이션 식별 시스템, 정밀 과금 정보 수집 및 측정 시스템 등의 URL, ACL 가속 NIC 기능을 제공할 수 있다. 나아가, 네트워크 가상화 기반의 클라우드 데이터 센터(Cloud Data Center)에서 클라우드 서버 시스템의 네트워크 보안 가속 NIC 기능을 제공할 수 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명의 일 실시 예에 따른 네트워크 보안 및 정보 보안 가속을 위한 NIC의 개념도,

도 2는 본 발명의 일 실시 예에 따른 NIC의 하드웨어 구조도,

도 3은 본 발명의 일 실시 예에 따른 NIC의 하드웨어 외관도,

도 4는 본 발명의 일 실시 예에 따른 멀티 코어 프로세서의 구조도,

도 5는 본 발명의 일 실시 예에 따른 범용 네트워크 컨트롤러의 내부 구조도,

도 6은 본 발명의 일 실시 예에 따른 DPDK와 NUMA를 이용한 NIC와 보안 어플리케이션 간의 고속 패킷 송수신 프로세스를 도시한 참조도,

도 7은 본 발명의 일 실시 예에 따른 고속 병렬 패킷 처리 성능을 지원하기 위한 패킷 부하 분산 기술을 설명하기 위한 참조도,

도 8은 본 발명의 일 실시 예에 따른 네트워크 보안 가속을 위한 멀티 코어 프로세서를 내장한 NIC를 장착한 네트워크 보안 및 정보보호 어플라이언스 시스템의 구조도,

도 9는 본 발명의 일 실시 예에 따른 SSL 암복호화를 위한 HTTPS 프록시 가속 프로토콜 스택의 구조도,

도 10은 본 발명의 일 실시 예에 따른 PCRE/YARA 패턴 매칭 가속을 설명하기 위한 PCRE/YARA Construct 구조도,

도 11은 본 발명의 일 실시 예에 따른 가상 머신에 대한 가상 오픈 스위치(Open vSwitch: OvS) 가속 오프로드 구조도,

도 12는 본 발명의 일 실시 예에 따른 DPDK 공개 소프트웨어를 이용한 어플리케이션 구조 및 기능을 도시한 참조도,

도 13은 본 발명의 일 실시 예에 따른 SSL 암복호화 기능 내장형 NIC를 기존의 SSL 암복호화 기능 독립형 장비와 비교한 참조도이다.

발명을 실시하기 위한 구체적인 내용

[0017] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시 예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시 예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시 예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0018] 본 발명의 실시 예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이며, 후술되는 용어들은 본 발명의 실시 예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0019] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들(실행 엔진)에 의해 수행될 수도 있으며, 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다.

[0020] 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다.

[0021] 그리고 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명되는 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0022] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능들을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있으며, 몇 가지 대체 실시 예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하며, 또한 그 블록들 또는 단계들이 필요에 따라 해당하는 기능의 역순으로 수행되는 것도 가능하다.

[0023] 이하, 첨부 도면을 참조하여 본 발명의 실시 예를 상세하게 설명한다. 그러나 다음에 예시하는 본 발명의 실시 예는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 다음에 상술하는 실시 예에 한정되는 것은 아니다. 본 발명의 실시 예는 이 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위하여 제공된다.

[0024] 도 1은 본 발명의 일 실시 예에 따른 네트워크 보안 및 정보 보안 가속을 위한 네트워크 인터페이스 카드(Network Interface Card: NIC, 이하 'NIC'라 칭함) 의 개념도이다.

[0025] 일 실시 예에 따른 NIC(1)는 네트워크 인터페이스(10), 멀티 코어 프로세서(12) 및 범용 네트워크 컨트롤러(14)를 포함하여, 멀티 코어 프로세서(12) 및 범용 네트워크 컨트롤러(14)로 구성된 하이브리드 구조를 가진다.

[0026] 네트워크 인터페이스(10)는 네트워크와 인라인 연결되어 네트워크로부터 트래픽을 입력받으며, 멀티 10기가(Gbps) 급 네트워크 인라인 회선을 수용한다. 예를 들어, 네트워크 인터페이스(10)는 네트워크 이중화와, 대용량 비대칭 회선에 적용할 수 있는 10Gbps 이더넷(ethernet) 2 회선(4 포트)을 가진다.

[0027] 멀티 코어 프로세서(12)는 보안 가속을 위한 프로세서로서, NIC(1)에 임베디드 되어, 네트워크 보안 및 정보보호 기능을 가속화한다. 고성능 네트워크 보안 및 정보보호 가속의 예로서, 트래픽 암복호화 가속 기능, 패턴 매칭 가속 기능, 보안 필터 가속 기능 등이 있다. 네트워크 보안 및 정보보호 가속을 위해, NIC(1)는 멀티 코어 프로세서(12)에, 트래픽 암복호화 기능, 패턴 매칭 기능 및 보안 가속 기능을 가진 네트워크 보안 가속엔진을 임베디드 시킨다.

[0028] 범용 네트워크 컨트롤러(14)는 데이터 플레인 개발 키트(Data Plane Development Kit: DPDK, 이하 'DPDK'라 칭함)를 지원하는 소프트웨어 개발 키트(Software Development Kit: SDK, 이하 'SDK'라 칭함)를 제공한다. 범용 네트워크 컨트롤러(14)는 업계 표준인 DPDK 기반의 고속 병렬 패킷 처리를 위해 DPDK 최적화를 지원한다.

[0029] 네트워크 보안 및 정보보호 어플리케이션(2)은 불균일 메모리 접근(Non-Uniform Memory Access: NUMA, 이하 'NUMA'라 칭함)과 같은 멀티 코어 프로세서의 병렬 처리 기술에 기반을 둔 서버 프로세서 환경에서, NIC(1)로부터 입력되는 패킷들을 코어 별로 분산시킬 수 있는 공개 소프트웨어인 DPDK 오픈 라이브러리(30) 기반의 부하 분산 기술을 제공한다.

[0030] 본 발명은 전술한 기능들을 통해 고성능 네트워크 보안을 보장하고, 정보보호 어플라이언스의 핵심 기능을 제공할 수 있다. NIC(1)는 보안 가속 기능을 통합 지원함에 따라, 기존의 단순 네트워크 접속 기능만을 수행하는 저가의 일반 NIC와는 달리 지능화의 개념을 적용한 고성능 네트워크 보안 가속을 지원할 수 있다. 나아가, 서버 시스템을 기반으로 하는 다양한 네트워크 응용 어플라이언스 제품의 핵심 부품으로 적용되어, 시스템의 패킷 처

리 성능 및 기능을 개선할 수 있다.

[0031] 도 2는 본 발명의 일 실시 예에 따른 NIC의 하드웨어 구조도이고, 도 3은 NIC의 하드웨어 외관도이다.

[0032] 도 2 및 도 3을 참조하면, NIC(1)는 ① 멀티 10기가급 네트워크 인라인 회선을 수용한다. 예를 들어, NIC(1)는 네트워크 이중화, 대용량 비대칭 회선에 적용할 수 있는 10Gbps 2 회선(4 포트)을 수용할 수 있다. 네트워크 인터페이스(10)가 IEEE-802.3, 10Gbps 이더넷 4 포트를 지원하고, 네트워크 인터페이스 타입은 SFP+이다. 호스트 접속 방식은 PCIe(PCI Express) Gen2/3 ×8/×4/×1 lane을 사용한다.

[0033] ② 일 실시 예에 따른 NIC(1)는 멀티 코어 프로세서(12)를 통해 네트워크 보안 및 정보보호 가속 기능을 제공한다. 네트워크 보안 및 정보보호 가속 기능 예로서, 패킷의 L2/3/4 및 L7 심층 패킷 분석 기술에 기반한 SSL(Secure Socket Layer) 암복호화 가속, PCRE(Perl Compatible Regular Expressions)/YARA 패턴 매칭 가속, ACL(Access Control List)/URL(Uniform Resource Locator) 필터 가속 기능을 지원한다. 네트워크 가상화 가속 기능의 예로서, 클라우드 가상 서버의 네트워크 인터페이스의 가상 오픈 스위치(Open vSwitch: OvS, 이하 OvS라 칭함) 가속 기능을 지원한다.

[0034] ③ 일 실시 예에 따른 NIC(1)는 DPDK 최적화를 위한 범용 네트워크 컨트롤러(14)를 통해 업계 표준인 DPDK를 기반으로 고속 병렬 패킷 처리를 지원한다. 범용 네트워크 컨트롤러(14)는 상용 이더넷 칩(IEEE 802.3 Ethernet MAC)으로서, DPDK 기반 가상 네트워크와 호스트 인터페이스를 제공한다. 예를 들어, NIC(1)는 DPDK 오픈 라이브러리(30)를 통해 네트워크 보안 및 정보보호 어플리케이션(2)과 패킷을 고속으로 송수신한다.

[0035] 도 4는 본 발명의 일 실시 예에 따른 멀티 코어 프로세서의 구조도이다.

[0036] 도 4를 참조하면, NIC에 내장되는 멀티 코어 프로세서(12)는 임베디드 소프트웨어 기반으로 유연한 구조의 고성능 네트워크 보안 오프로드 요구사항을 만족한다. 멀티 코어 프로세서(12)는 10Gbps 4 포트를 수용하고, 최대 40Gbps의 트래픽을 실시간으로 분석할 수 있는 프로세서 성능을 가진다.

[0037] 멀티 코어 프로세서(12)는 네트워크 보안 가속엔진(120)을 포함한다. 일 실시 예에 따른 네트워크 보안 가속엔진(120)은 암복호화 가속기(122), 패턴 매칭 가속기(124) 및 보안 필터 가속기(126)를 포함한다.

[0038] 암복호화 가속기(122)는 SSL 트래픽의 암호화(Encrypt)/복호화(Decrypt)를 가속화한다. 예를 들어, 암복호화 가속기(122)는 SSL 암복호화 가속 기능을 제공한다. 패턴 매칭 가속기(124)는 PCRE/YARA 패턴 매칭을 가속화한다. 패턴 매칭 가속기(124)는 사용자 정의 시그니처 패턴을 실시간으로 검색하기 위해, PCRE/YARA 표준에 호환되는 패턴 매칭 가속 기술을 사용한다. 패턴 매칭 가속기(124)의 PCRE/YARA 패턴 매칭 가속에 대해서는 도 10을 참조로 하여 후술한다.

[0039] 보안 필터 가속기(126)는 ACL/URL 필터 가속 기능을 지원한다. 네트워크 보안 시스템은 외부에서 유입되는 트래픽에 대한 L2/L3/L4/L7 계층으로 패킷 상세 분석을 수행하여 패킷의 악성 코드 감염 여부, 유해사이트 접근 여부를 판단해야 하며, 식별 결과에 따라 차단, 우회, 미러 등의 정책을 수행해야 한다. 본 발명에서는 멀티 코어 프로세서(12)의 보안 필터 가속기(126)를 이용하여 100만 엔트리 이상의 대용량 ACL 및 URL/IP 필터 가속 기능을 제공한다. 멀티 코어 프로세서(12)를 통해 네트워크 보안 가속의 안정성 및 성능을 확보할 수 있다.

[0040] 도 5는 본 발명의 일 실시 예에 따른 범용 네트워크 컨트롤러의 내부 구조도이다.

[0041] 도 5를 참조하면, 범용 네트워크 컨트롤러(14)는 상용 이더넷 칩셋을 채택하여 PCIe 입출력(I/O) 가속 기능을 제공한다. 고성능 멀티 CPU 서버의 네트워크 성능을 최대로 활용하기 위해 고속 병렬 패킷 처리를 위한 물리 기능(Physical Function: PF)과 가상 기능(Virtual Function: VF)을 지원한다. 범용 네트워크 컨트롤러(14)는 PCIe I/O 고속 병렬 패킷 처리 호스트 인터페이스를 제공하기 위해, 업계 표준으로 자리 잡은 DPDK와 호환되는 PCIe 인터페이스를 제공한다. 이에 따라, 기존 DPDK를 사용하는 네트워크 보안 어플리케이션에서 요구되었던 NIC 전용 디바이스 드라이버와 SDK 추가 개발 없이도 보안 가속 기능을 적용할 수 있다. 최근 서버 시스템과 멀티 코어 CPU 기술의 발전으로 서버 시스템의 멀티 코어를 활용하는 병렬 패킷 처리 라이브러리로 DPDK 오픈 라이브러리(DPDK open library)가 업계 표준으로 자리 잡고 있다. 본 발명은 보안 어플리케이션이 사용자 평면(user plane)의 DPDK 오픈 라이브러리를 통해 커널을 통과(pass)하여 직접 NIC에 액세스할 수 있음에 따라 고속 병렬 패킷 처리가 가능하다.

[0042] 일 실시 예에 따른 범용 네트워크 컨트롤러(14)는 PCIe 단일 루트 입출력 가상화(Single Root I/O Virtualization: SR-IOV, 이하 'SR-IOV'라 칭함) 기반의 네트워크 가상화를 지원하는 SR-IOV PCIe 엔드포인트(endpoint)(140)를 포함한다. SR-IOV PCIe 엔드포인트(140)는 PCIe Gen2/3 ×8/×4/×1 lane을 통해 호스트 메

모리(20)에 호스트 접속하여, 호스트 메모리(20)의 물리기능 객체(PF object)와 가상기능 객체(VF Object)에 접근한다. 가상화에서 SR-IOV는 관리 용이성 및 성능상의 이유로 PCIe 리소스를 격리할 수 있는 사양이다. 단일 물리적 PCIe는 SR-IOV 사양을 사용하여 가상환경에서 공유할 수 있다. SR-IOV는 물리적 서버 컴퓨터의 서로 다른 가상 구성 요소(예: 네트워크 어댑터)에 서로 다른 가상 기능을 제공한다. SR-IOV를 사용하면 가상환경의 여러 가상장치(VMs)가 단일 PCIe 하드웨어 인터페이스를 공유할 수 있다.

[0043] 도 6은 본 발명의 일 실시 예에 따른 DPDK와 NUMA를 이용한 NIC와 보안 어플리케이션 간의 고속 패킷 송수신 프로세스를 도시한 참조도로, 세부적으로, 도 6의 (a)는 종래 NIC와 보안 어플리케이션 간의 패킷 송수신 프로세스를 도시한 것이고, 도 6의 (b)는 본 발명의 일 실시 예에 따른 멀티 코어 프로세서가 내장된 NIC와 보안 어플리케이션 간의 고속 패킷 송수신 프로세스를 도시한 것이다.

[0044] 도 6을 참조하면, 일 실시 예에 따른 네트워크 시스템은 멀티 CPU 서버 시스템의 프로세서 자원을 최대한 활용하여 네트워크 보안 어플라이언스의 성능을 향상시키기 위해 DPDK 공개 소프트웨어를 이용한다. DPDK 공개 소프트웨어는 DPDK 오픈 라이브러리를 포함한다. 네트워크에서 수신된 패킷을 보안 어플리케이션으로 송수신함에 있어 시스템(예를 들어 리눅스 운영체제)의 스케줄링, 메모리 복사, 인터럽트 등의 부하를 제거하고, 보안 어플리케이션에 메모리와 CPU를 고정 할당하는 NUMA 방법으로 패킷을 분산 처리하여 최대의 성능을 얻을 수 있다.

[0045] 네트워크 시스템은 하드웨어 공간(Hardware Space)과, 운영 시스템 커널 공간(Operating System Kernel Space)과, 사용자 공간(User Space)으로 구분할 수 있다. 하드웨어 공간(Hardware Space)은 NIC를 포함하고, 운영 시스템 커널 공간(Operating System Kernel Space)은 네트워킹 모듈(Networking Module)과 디바이스 드라이버(Device Driver)를 포함하며, 사용자 공간(User Space)은 서버 기반 어플리케이션(예를 들어 보안 어플리케이션)을 포함한다.

[0046] 도 6의 (a)에 도시된 바와 같이, 종래 NIC는 보안 어플리케이션과의 패킷 송수신 시에, (1) 디바이스 드라이버 오버헤드, (2) 프로토콜 스택 오버헤드 및 (3)커널(Kernel)/사용자(User) 메모리 카피 오버헤드가 발생한다. 이에 따라, 서버 CPU의 패킷 처리 성능에 한계가 발생한다. 이에 비해, 도 6의 (b)에 도시된 바와 같이, 일 실시 예에 따른 NIC(1)는 범용 네트워크 컨트롤러의 패킷 처리 엔진을 통해 PCIe I/O, 커널의 스케줄링, 메모리 복사, 인터럽트 등의 부하를 제거한다. NIC(1)는 멀티 코어 프로세서의 네트워크 보안 가속엔진을 통해 패킷 처리 부하를 오프로드(offload) 한다. 네트워크 보안 가속엔진은 필터링(filtering), 컬러링(Coloring), 샘플링(Sampling), 패턴 매칭(Pattern Matching), TCP/IP 오프로드(TCP/IP offload), 고정밀 심층 패킷 분석(Deep Packet Inspection: DPI, 이하 'DPI'라 칭함) 오프로드(DPI offload) 등을 수행한다. 이때, DPI 기술에 기반한 SSL 암복호화, PCRE 패턴 매칭과 같은 핵심 네트워크 보안 기술을 NIC와 같은 반제품으로 오프로드하여 완제품에 해당하는 어플라이언스 시스템 성능과 용량을 높인다.

[0047] DPDK는 고성능 패킷처리 최적화를 위한 시스템 소프트웨어로서, 크게 DPDK 오픈 라이브러리(DPDK open Library)와, 패킷 처리 최적화를 위한 DPDK 디바이스 드라이버(DPDK device driver)의 집합으로 구성되어 있다. DPDK는 기존 리눅스 기반의 패킷처리과정처럼 커널에서 패킷처리과정을 거치는 것(도 6의 (a) 참조)이 아니라 보안 어플리케이션(2)이 사용자 공간의 DPDK 오픈 라이브러리(30)와 EAL(Environment Abstraction Layer)을 사용하여 커널을 통과하여 직접 NIC(1)에 액세스할 수 있는 통로를 제공한다는 것이다. DPDK는 사용자 평면의 DPDK 오픈 라이브러리(30)뿐만 아니라, 패킷처리에 최적화된 DPDK 디바이스 드라이버를 제공한다(도 6의 (b) 참조).

[0048] 일 실시 예에 따른 네트워크 시스템은 보안 어플리케이션(2)에 메모리와 CPU를 고정 할당하는 NUMA 방법으로 패킷을 분산 처리하여 최대의 성능을 얻을 수 있다. 도 6의 (b)에 도시된 바와 같이, DPDK와 NUMA를 이용하여 패킷을 분산 처리함에 따라, (1) 디바이스 드라이버 및 프로토콜 스택 오버헤드를 제거하고, (2) NUMA 메모리 관리 구조를 적용할 수 있다.

[0049] 도 7은 본 발명의 일 실시 예에 따른 고속 병렬 패킷 처리 성능을 지원하기 위한 패킷 부하 분산 기술을 설명하기 위한 참조도이다.

[0050] 도 7을 참조하면, 일 실시 예에 따른 NIC는 DPDK를 이용한 고속 병렬 패킷 처리 네트워크 인터페이스를 제공한다. 멀티 CPU 서버 시스템의 멀티 코어 프로세서를 이용한 고속 병렬 패킷 처리를 위해, NIC는 RSS(Receiver Side Scaling)(도 7의 (a))와 DCB(Data Center Bridging)(도 7의 (b)) 기능을 지원하여 네트워크로부터 수신된 패킷을 서버 시스템의 멀티 코어 프로세서로 분배할 수 있어야 한다. RSS는 NIC 내에 L4 파서를 이용하여 5-튜플 해시 값을 계산하고, 플로우 별로 수신 코어를 지정한다.

[0051] 도 8은 본 발명의 일 실시 예에 따른 네트워크 보안 가속을 위한 멀티 코어 프로세서를 내장한 NIC를 장착한 네

트워크 보안 및 정보보호 어플라이언스 시스템의 구조도이다.

[0052] 도 8을 참조하면, 네트워크 보안 및 정보보호 어플라이언스 시스템은 NIC(1)와, 네트워크 보안 및 정보보호 어플리케이션 서버(2)를 포함한다. NIC(1)는 보안 가속을 위한 멀티 코어 프로세서(12)와, 범용 네트워크 컨트롤러(14)를 포함한다. 도 8에서는 NIC(1)를 최대 2개까지 장착하여 최대 80기가 급의 네트워크 보안 어플라이언스 확장 구조를 도시하고 있다.

[0053] NIC(1)는 10Gbps 8 포트를 수용할 수 있다. NIC(1)의 멀티 코어 프로세서(12)는 SSL 암복호화, PCRE 패턴 매칭과 같은 보안 가속 기능을 오프로드한다. 범용 네트워크 컨트롤러(14)는 SR-IOV를 지원하며, DPDK에 최적화된다. 네트워크 보안 및 정보보호 어플리케이션 서버(2)의 멀티 코어 프로세서를 이용하여 수신 패킷을 병렬 처리함에 따라 최적의 성능 구조를 만족할 수 있다. 네트워크 보안 및 정보보호 어플리케이션 서버(2)는 네트워크 보안 및 정보보호를 위한 것으로, 멀티 코어 프로세서를 이용하여 수신 패킷을 병렬 처리한다. 이때, 각 멀티 코어 프로세서는 DPDK와 NUMA를 이용하여 패킷을 분산 처리한다.

[0054] 도 9는 본 발명의 일 실시 예에 따른 SSL 암복호화를 위한 HTTPS 프록시 가속 프로토콜 스택의 구조도이다.

[0055] 도 9를 참조하면, NIC에 내장된 보안 가속을 위한 멀티 코어 프로세서는 AES(Advanced Encryption Standard), DES(Data Encryption Standard), 3DES와 같은 대칭 암호화(Symetric Crypto)와, MD-5, SHA, Kasumi와 같은 해싱 알고리즘을 가속하는 암복호화 가속기를 이용하여 SSL 암복호화 가속 기능을 제공한다. 또한, 웹 성능 확보를 위한 사용자 공간(User Space)에서 동작하는 고성능 TCP/IP 스택을 가지는 HTTPS 프록시를 제공한다. HTTPS 프록시는 클라이언트(예를 들어, SSL 클라이언트)와 웹 서버(예를 들어, SSL 서버) 사이에서 대리하는 기능을 수행한다. 예를 들어, SSL로 암호화된 HTTPS 통신을 클라이언트와 웹 서버 사이에서 대리한다.

[0056] SSL은 "넷스케이프(Netscape)" 사에서 개발한 암호화 프로토콜로서, 현재 인터넷 전자상거래 등 금융거래 정보 및 개인정보 등의 안전한 데이터 통신을 위한 사실상의 표준 프로토콜이다. SSL3.0 버전부터 IETF(Internet Engineering Task Force)에 의해 표준화되어 TLS(Transport Layer Security)로 명명되었다. 즉, SSL 3.0과 TLS 1.0은 같은 프로토콜이다. SSL은 TCP/IP 기반의 모든 응용 프로토콜에 이용될 수 있지만, 최근 주로 사용되는 대표적인 응용 프로토콜로서 HTTPS가 있다. HTTPS는 종래의 HTTP 프로토콜의 데이터 통신 패킷을 SSL을 이용하여 전송 계층(Transport Layer)에서 암호화하여 송수신하는 일종의 HTTP 변형 프로토콜이다.

[0057] 도 10은 본 발명의 일 실시 예에 따른 PCRE/YARA 패턴 매칭 가속을 설명하기 위한 PCRE/YARA Construct 구조도이다.

[0058] 침입 탐지 시스템(IPS/IDS), 정보보호 또는 APT와 같은 네트워크 보안 시스템은 Zero-day 공격에 방어할 수 있도록 사용자 정의 시그니처 패턴을 실시간으로 탐지하는 기능이 필수적으로 요구되고 있다. 본 발명에서는 사용자 정의 패턴을 10 Gbps 속도로 실시간 검색할 수 있도록 PCRE/YARA 표준에 호환되는 패턴 매칭 가속 기술을 제안한다. 일반적으로 패턴 매칭 방법에는 DFA(Deterministic Finite Automata), NFA(Nondeterminstic Finite Automata) 알고리즘이 사용되고 있다. 본 발명에서는 멀티 코어 프로세서에 내장된 HFA(Hyper Finite Automata) 패턴 매칭 전용 프로세서를 이용하여 고속 실시간 PCRE/YARA 패턴 매칭 성능을 지원한다. 본 발명에서는 산업 표준으로 사용되는 PCRE Construct(도 10의 (a))와, YARA Construct(도 10의 (b))를 지원한다.

[0059] 도 11은 본 발명의 일 실시 예에 따른 가상 머신에 대한 가상 오픈 스위치(Open vSwitch: OvS, 이하 OvS라 칭함) 가속 오프로드 구조도이다.

[0060] 일 실시 예에 따른 NIC(1)는, 시스템 가상화를 위한 하이퍼바이저 환경에서 구동되는 가상 장치(Virtual Machine: VM)와 코어 및 메모리를 공유한다. 이때, 성능적으로 부하가 발생하는 커널 기반의 OvS 기능을, NIC(1)에 내장된 SR-IOV 하드웨어 기술과 멀티 코어 프로세서를 이용해서 오프로딩하여 다음과 같은 기능을 제공한다. NIC(1)는 분산 가상 스위치 기능을 제공한다. 즉, 다른 물리 서버에 위치한 가상 장치(VM)와 서로 연결한다. 또한, NIC(1)는 오픈 플로우 프로토콜(Open Flow Protocol) 기반의 원격 제어를 지원하고, 가상 장치(VM)별로 트래픽 분리(traffic isolation)를 지원하며, 터널링 프로토콜을 지원한다. 예를 들어, GRE, VXLAN, IPsec 등을 지원한다. 또한, 모니터링 기능을 지원한다. 예를 들어, NetFlow, sFlow, IPFIX 등을 지원한다.

[0061] 도 12는 본 발명의 일 실시 예에 따른 DPDK 공개 소프트웨어를 이용한 어플리케이션 구조 및 기능을 도시한 참조도이다.

[0062] 일 실시 예에 따른 NIC(1)는 멀티 코어 프로세서와 범용 네트워크 컨트롤러가 하이브리드된다. NIC(1)는 보안 가속을 위한 멀티 코어 프로세서와 범용 네트워크 컨트롤러를 하이브리드하게 채택하여 다음과 같은 경쟁 우위

를 가진다. 예를 들어, 40Gbps 성능을 지원하는 트래픽 처리 이원화를 지원한다. 즉, 멀티 코어 프로세서를 제공하여 트래픽을 전처리(예를 들어, 암호화 패킷 처리, 트래픽 감시)하고, 범용 네트워크 컨트롤러를 이용하여 트래픽을 후처리(예를 들어, DPDK 최적화) 하여 호스트 시스템과 연동한다. 또한, NIC(1)는 네트워크 보안에 필수적인 SSL 암복호화, PCRE 패턴매칭, 오픈 플로우 컨트롤러 기능을 NIC(1)로 오프로드하여 설치 공간 절약 및 빠른 응답속도를 확보할 수 있다. 나아가, 리눅스, 윈도즈 등의 운영체제와 상관없이 별도의 드라이버 설치나 변경 없이 설치 및 통합이 가능하다.

[0063] 본 발명은 NIC(1)에 내장된 임베디드 멀티 코어 프로세서 기반 네트워크 보안 하드웨어 가속 기술을 제공한다. 본 발명의 핵심 기술로는 SSL 암복호화, PCRE 패턴 매칭과 같이 성능 부하를 유발하는 네트워크 보안 기능을 시스템에 장착된 NIC의 멀티 코어 프로세서로 임베디드 시켜 보안 기능을 오프로드 하는 기술이다. 본 발명의 네트워크 보안 가속 기능은 인라인 모드에서 입력되는 SSL 암호화 패킷을 포함하여 TCP Stateful 플로우를 추적하고, 필요 시 암복호화하여 전송되는 내용 중에 RegEx으로 표현되는 PCRE/YARA 시그니처가 존재하는지를 실시간으로 찾아내는 패턴 매칭 기능을 수행하는 로직을 임베디드 멀티 코어 프로세서의 가속기와 연계해서 고속의 패킷 처리 성능을 제공한다.

[0064] 본 발명은 DPDK 공개 소프트웨어(3) 기반의 고속 병렬 패킷 처리 어플리케이션 소프트웨어 기술을 제공한다. 최근 서버 시스템과 멀티 코어 CPU 기술의 발전으로 시스템의 멀티 코어를 활용하는 병렬 패킷 처리 라이브러리로 DPDK 공개 소프트웨어(3)가 업계 표준으로 자리 잡고 있다. 본 발명에서는 NIC가 범용 네트워크 컨트롤러로서 상용 이더넷 칩셋을 채택하여 DPDK와 호환되는 PCIe 인터페이스를 제공하여 기존 DPDK를 사용하는 네트워크 보안 및 정보 보호 어플리케이션(2)에서 NIC 전용 디바이스 드라이버, SDK 추가 개발 없이 보안 가속 기능을 이용할 수 있다. 도 12에 도시된 바와 같이 DPDK 공개 소프트웨어(3)의 DPDK 오픈 라이브러리(30)를 통해, 서버 기반 네트워크 보안 및 정보보호 어플리케이션(2)이 커널(Kernel)을 통과하여 직접 NIC(1)에 액세스할 수 있도록 한다.

[0065] 도 13은 본 발명의 일 실시 예에 따른 SSL 암복호화 기능 내장형 NIC를 기존의 SSL 암복호화 기능 독립형 장비와 비교한 참조도이다.

[0066] 도 13을 참조하면, 도 13의 (a)에 도시된 바와 같이 기존의 네트워크 시스템은 SSL 암복호화 장비가 별도로 분리되어 있었다. 그러나 일 실시 예에 따른 네트워크 시스템은 도 13의 (b)에 도시된 바와 같이 SSL 암복호화 기능이 NIC에 내장된다. 예를 들어, SSL 암호화된 트래픽을 NIC에 내장된 멀티 코어 프로세서를 사용하여 복호화한다. 이를 위해, NIC에 SSL 복호화 기능이 오프로딩 된다. 본 발명은 NIC에서 SSL 암복호화를 지원하여 하나의 어플라이언스에서 통합 지원되는 방식을 제공한다.

[0067] 다른 실시 예에 따른 NIC는 멀티 코어 프로세서 기반의 보안 가속을 달성한다. 예를 들어, 멀티 10기가급 이더넷 네트워크를 대상으로 PCRE/YARA 기반 패턴 매칭 가속 기능을 지원하는 네트워크 보안 기술을 단일 NIC 내에 임베디드 멀티 코어 프로세서 기술을 사용하여 구현한다. 다양한 네트워크 보안 기능을 가속하는 NIC로 네트워크 보안 분야에서 경쟁력을 가질 수 있을 것이다.

[0068] 도 1 내지 도 13을 참조로 하여 전술한 바에 따라, 본 발명은 다음과 같은 효과를 달성할 수 있다.

[0069] 차세대 NIC로서 고부가가치 기술 개발 효과가 있다. 본 발명에 따르면, SSL 암복호화, PCRE 패턴 매칭, PCIe I/O 무손실 데이터 전달을 위한 I/O 가속 등과 같은 고급 기술 사양을 NIC 내에서 제공한다. 이러한 가속 기능은 메인 프로세서의 과도한 부하를 유발하는데, 이 기능을 NIC에 오프로드한다. 이에 따라, 종래의 단순한 네트워크 접속 기능만을 지원하는 NIC와는 한 차원 다른 새로운 개념의 차세대 제품이 될 것으로 기대하고 있다. 네트워크 보안 분야에서 고부가가치 영역에 속하는 고성능 네트워크 보안 어플라이언스 제품군에 사용되는 제품이 될 것이다.

[0070] 네트워크 보안, 정보보호 제품의 경쟁력 저하의 주원인은 서버 시스템 구조와 소프트웨어에만 의존하기 때문이다. 본 발명은 NIC에 장착되는 하드웨어 기술에 의한 성능 가속 기술을 통해 이를 해결하고자 한다. 본 발명은 10기가급 네트워크 2회선까지 수용할 수 있는 대용량 고속 네트워크 인터페이스 기술로서, 웹 방화벽, IDS, IPS, DLP, 방화벽 장비의 개발 오버헤드를 줄인다. 성능과 기능에서 경쟁력을 갖게 하여 고부가 가치 네트워크 보안 어플라이언스 장비로 경쟁 우위를 확보할 수 있다.

[0071] 본 발명은 네트워크 보안 솔루션의 암호화 트래픽 가시화 기반 기술로 활용될 수 있다. 본 발명은 고속의 암호화 트래픽 복호화 기술을 적용한 것으로, SSL 암호화 트래픽을 복호화하여 내부의 위협을 차단할 수 있다. 현재 보안 시스템의 상당 수가 SSL 트래픽 내부의 위협을 인식하거나 차단하지 못하고 있으며 자체 솔루션이 아닌 어

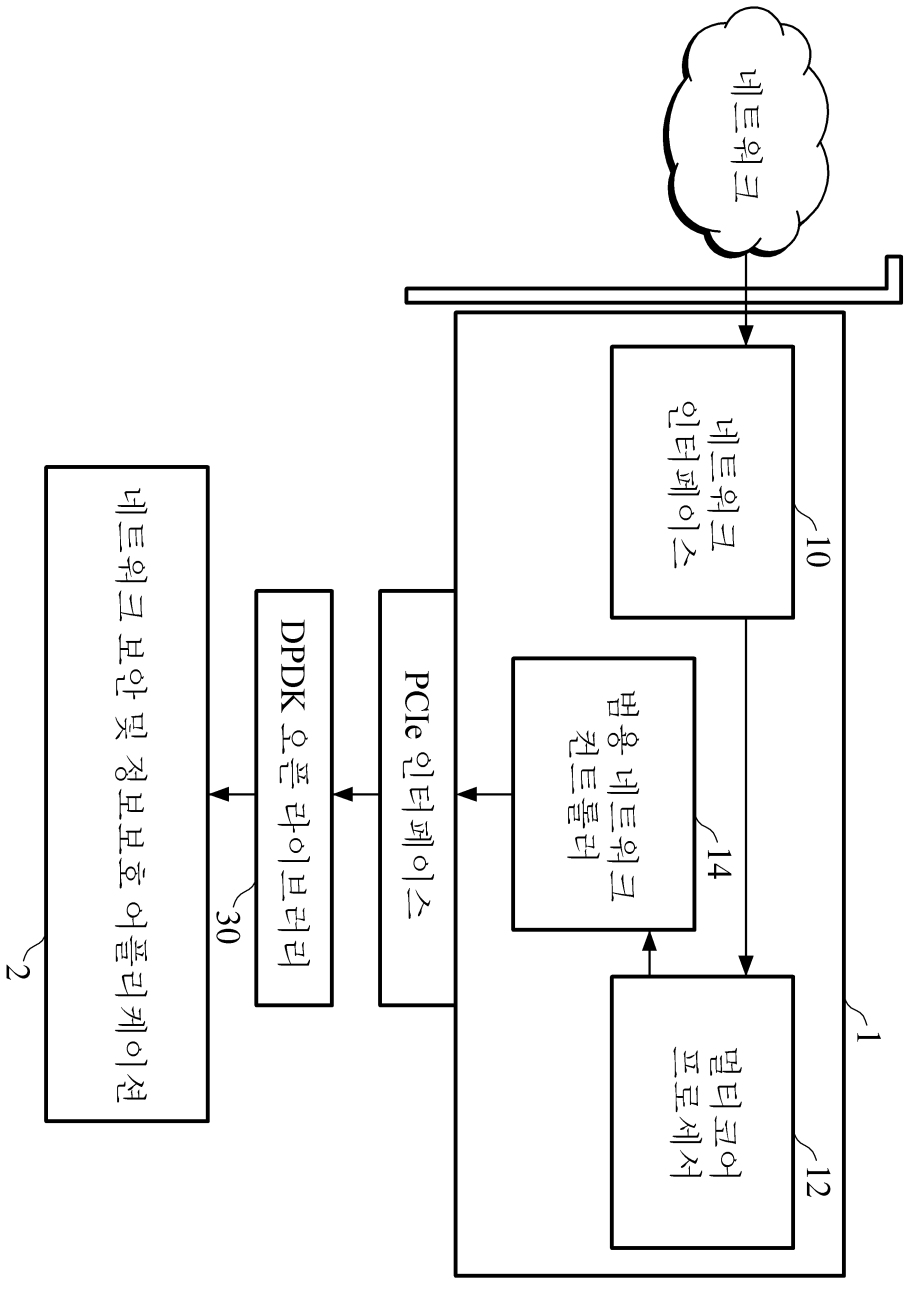
플라이언스 형태의 SSL 복호화 솔루션을 함께 구성하여 보안 서비스가 이루어지고 있다. 따라서, SSL 복호화 기능이 제공되는 멀티 기가급 NIC는 기존 네트워크 보안 솔루션의 중요한 기반 기술로 활용될 것이다.

[0072] 본 발명은 클라우드 기반 네트워크 가상화 플랫폼의 기반 기술로 활용될 수 있다. 본 발명은 네트워크 기능 가상화(Network Function Virtualization: NFV) 아키텍처 기반의 인프라스트럭처 플랫폼에 적용 가능한 OvS(Open vSwitch) 기능을 오프로드하는 기술을 제공한다. 데이터센터의 네트워크 운영 비용을 절감하고 새로운 부가가치 서비스를 신속하게 구현하기 위한 가상화된 네트워크 기능(Virtualized Network Function: VNF)을 구현하는 인프라스트럭처 플랫폼 내에서 핵심적인 기능을 담당하게 될 것이다.

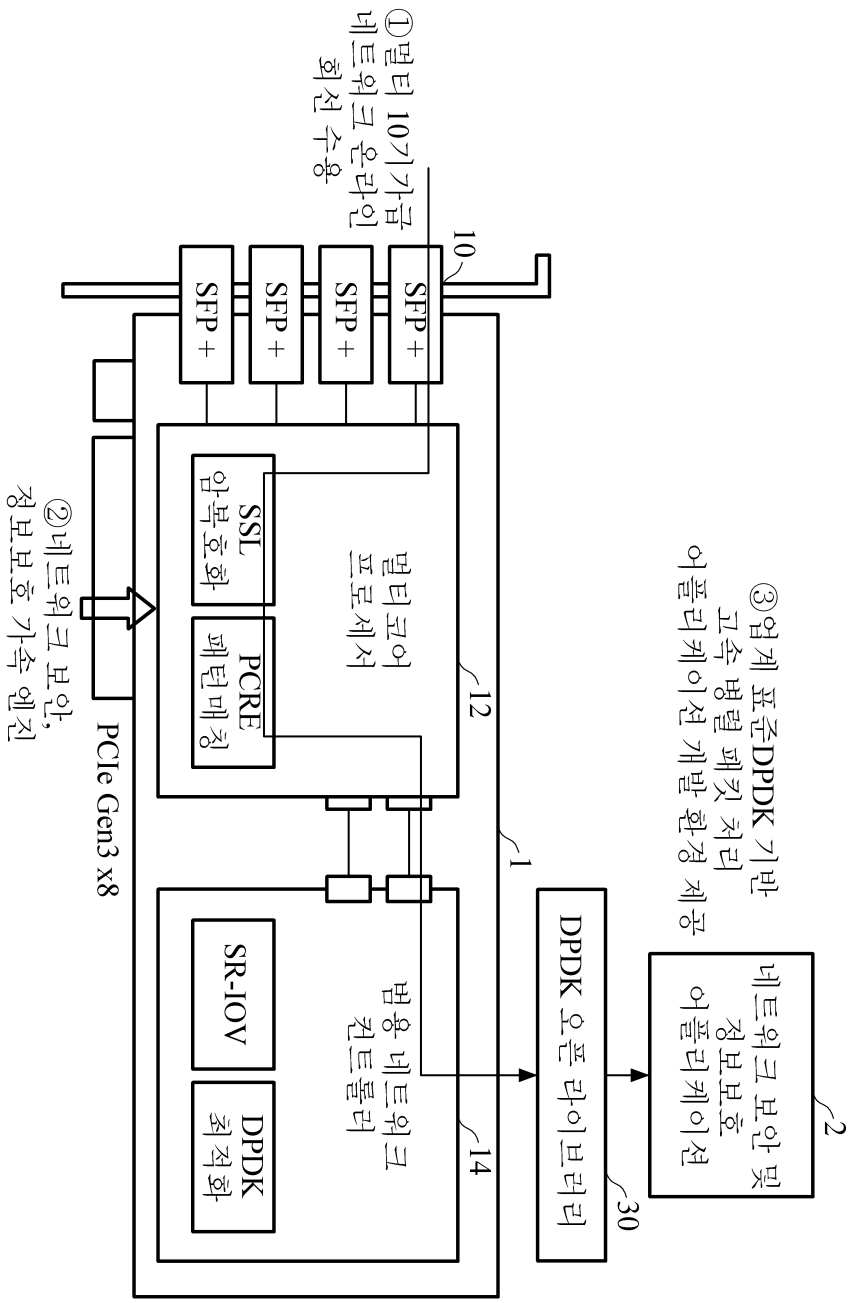
[0073] 이제까지 본 발명에 대하여 그 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시 예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

도면

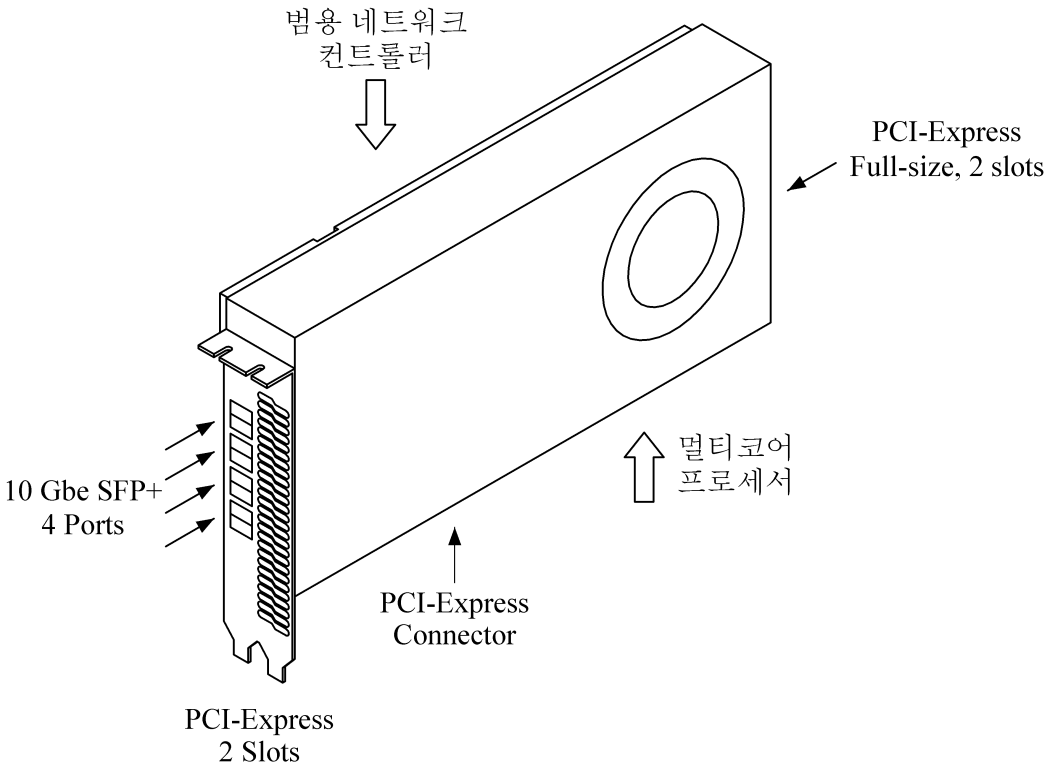
도면1


네트워크
네트워크 인터페이스
10
범용 네트워크 컨트롤러
14
멀티코어 프로세서
12
1
PCIe 인터페이스
DPDK 오픈 라이브러리
30
네트워크 보안 및 정보보호 어플리케이션
2

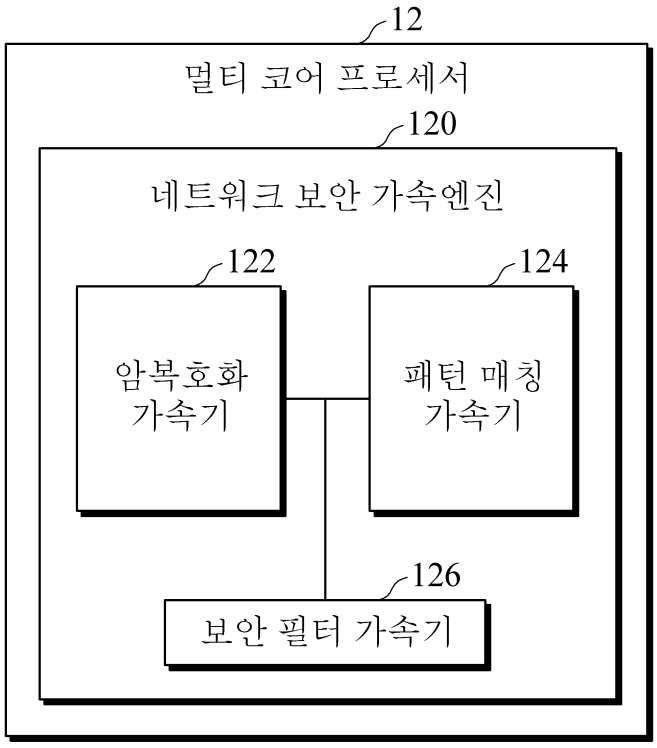
도면2


①멀티 10기가급
네트워크 온라인
회선 수용
10
SFP +
SFP +
SFP +
SFP +
②네트워크 보안,
정보보호 가속 엔진
PCIe Gen3 x8
멀티 코어
프로세서
SSL
암복호화
PCRE
패턴매칭
12
범용 네트워크
컨트롤러
SR-IOV
DPDK
최적화
14
1
③업계 표준DPDK 기반
고속 병렬 패킷 처리
어플리케이션 개발 환경 제공
DPDK 오픈 라이브러리
30
네트워크 보안 및
정보보호
어플리케이션
2

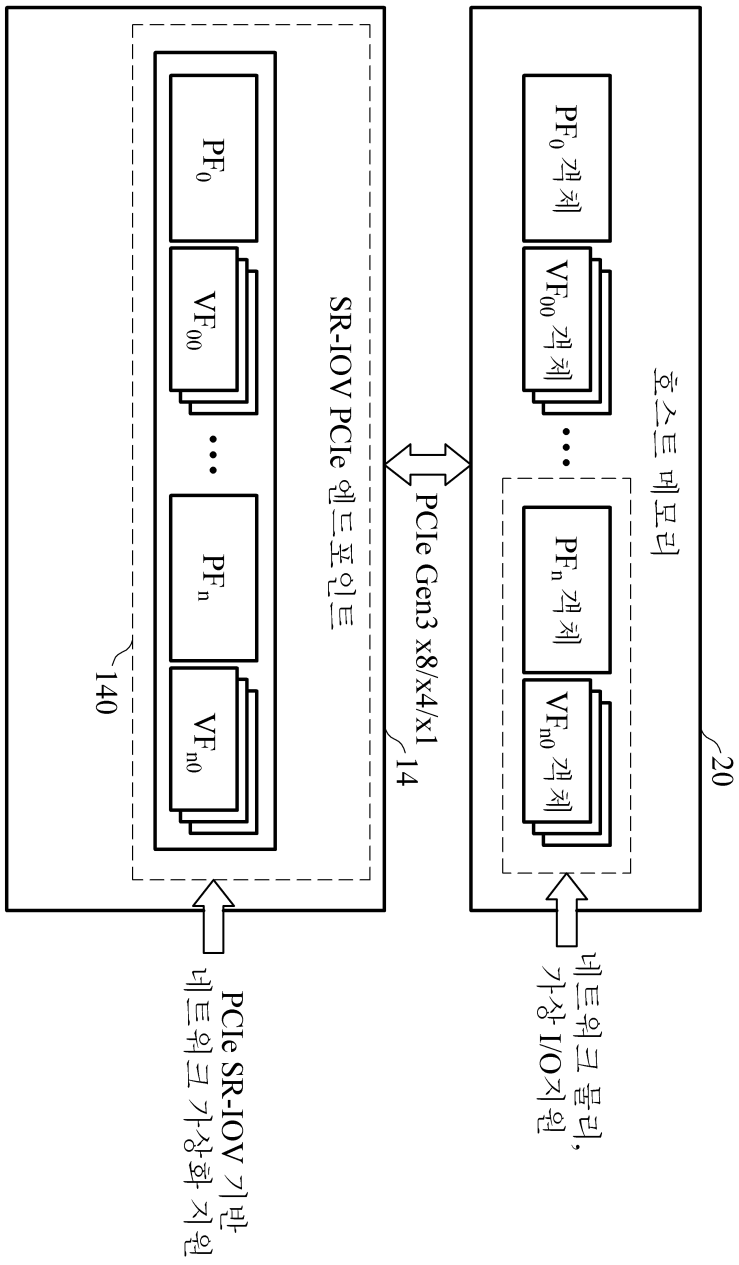
도면3


범용 네트워크
컨트롤러
PCI-Express
Full-size, 2 slots
멀티코어
프로세서
10 Gbe SFP+
4 Ports
PCI-Express
Connector
PCI-Express
2 Slots

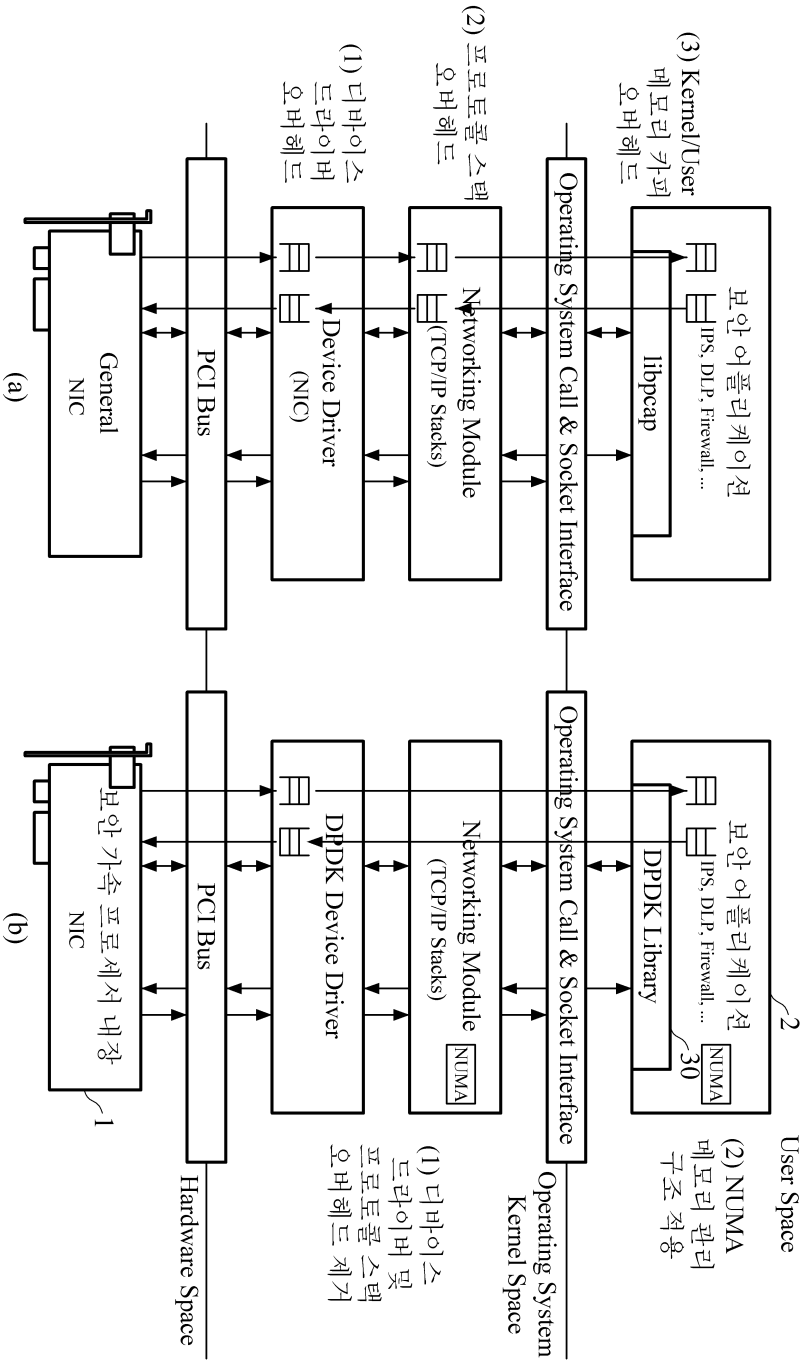
도면4


12
멀티 코어 프로세서
120
네트워크 보안 가속엔진
122
124
암복호화
가속기
패턴 매칭
가속기
126
보안 필터 가속기

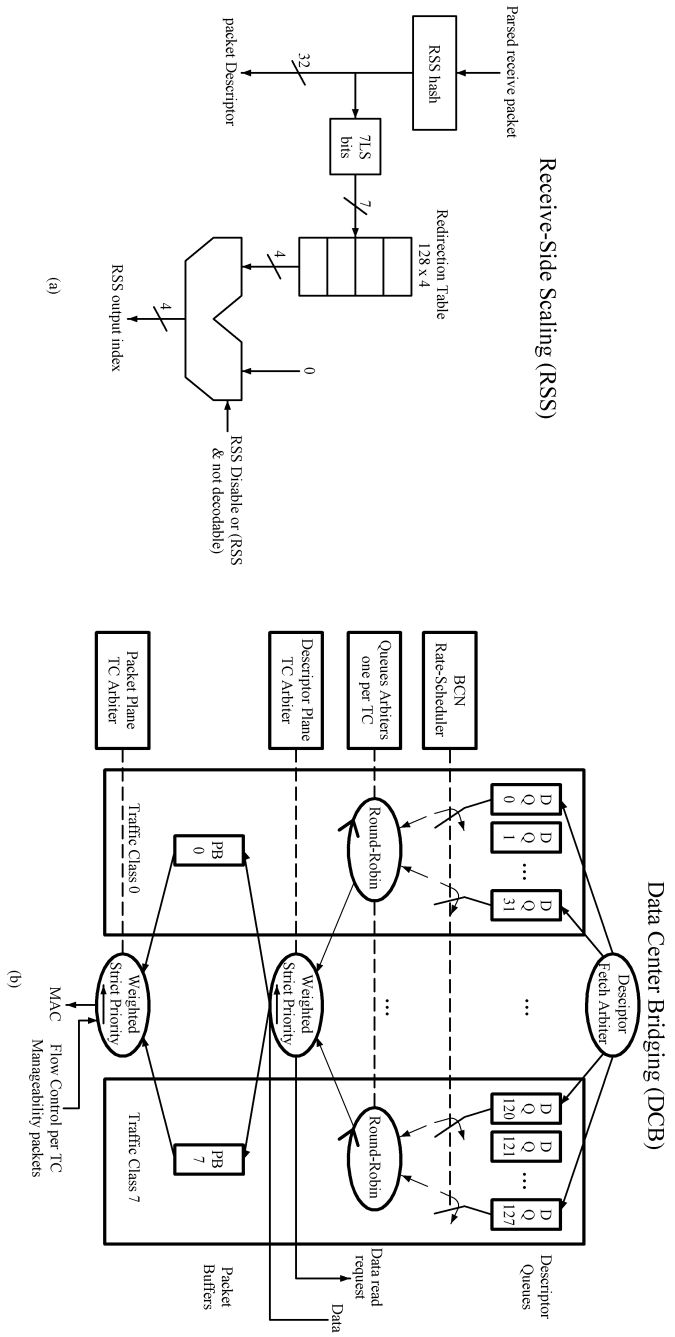
도면5


호스트 메모리
PF0 객체
VF00 객체
PFn 객체
VFn0 객체
20
네트워크 물리,
가상 I/O지원
PCIe Gen3 x8/x4/x1
14
SR-IOV PCIe 엔드포인트
PF0
VF00
PFn
VFn0
140
PCIe SR-IOV 기반
네트워크 가상화 지원

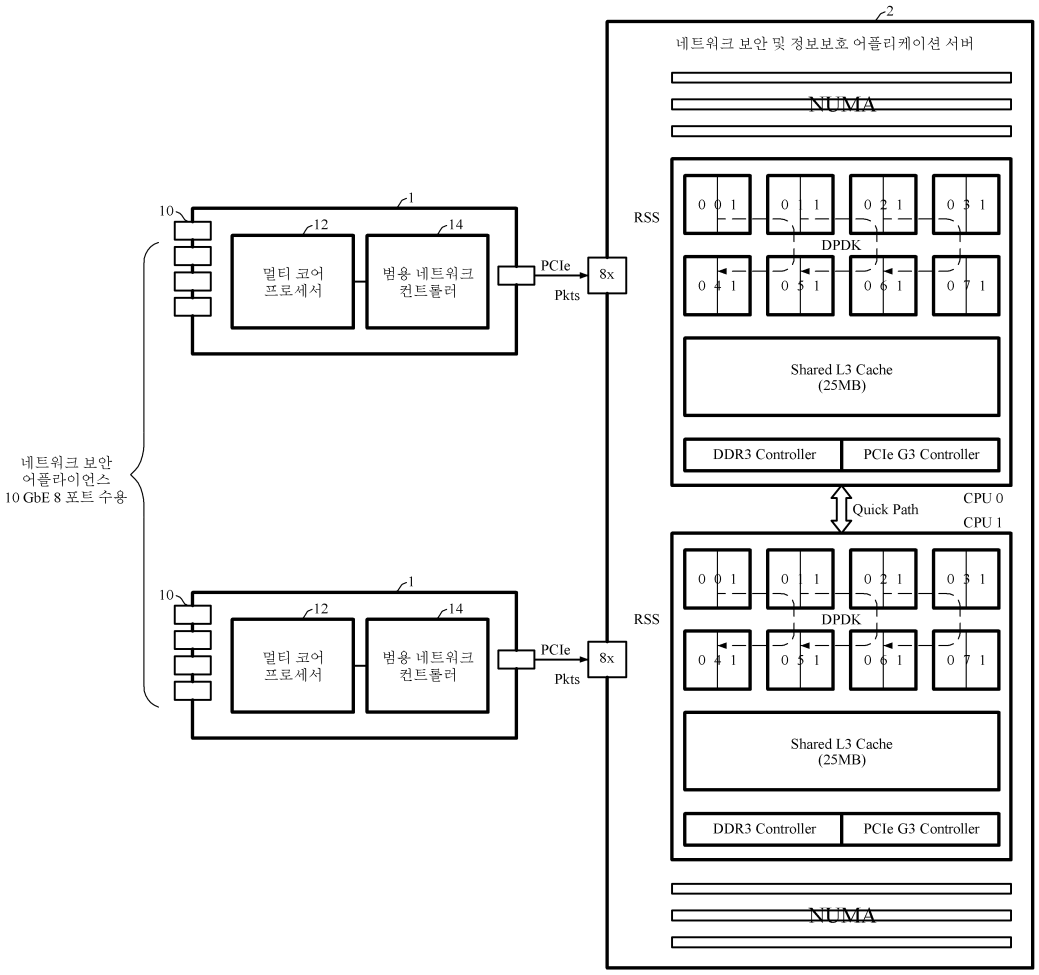
도면6


User Space
Operating System
Kernel Space
Hardware Space
보안 어플리케이션
IPS, DLP, Firewall, ...
libpcap
DPDK Library
NUMA
2
30
(2) NUMA
메모리 관리
구조 적용
(3) Kernel/User
메모리 카피
오버헤드
Operating System Call & Socket Interface
(2) 프로토콜 스택
오버헤드
Networking Module
(TCP/IP Stacks)
(1) 디바이스
드라이버
오버헤드
Device Driver
(NIC)
DPDK Device Driver
(1) 디바이스
드라이버 및
프로토콜 스택
오버헤드 제거
PCI Bus
General
NIC
(a)
보안 가속 프로세서 내장
NIC
1
(b)

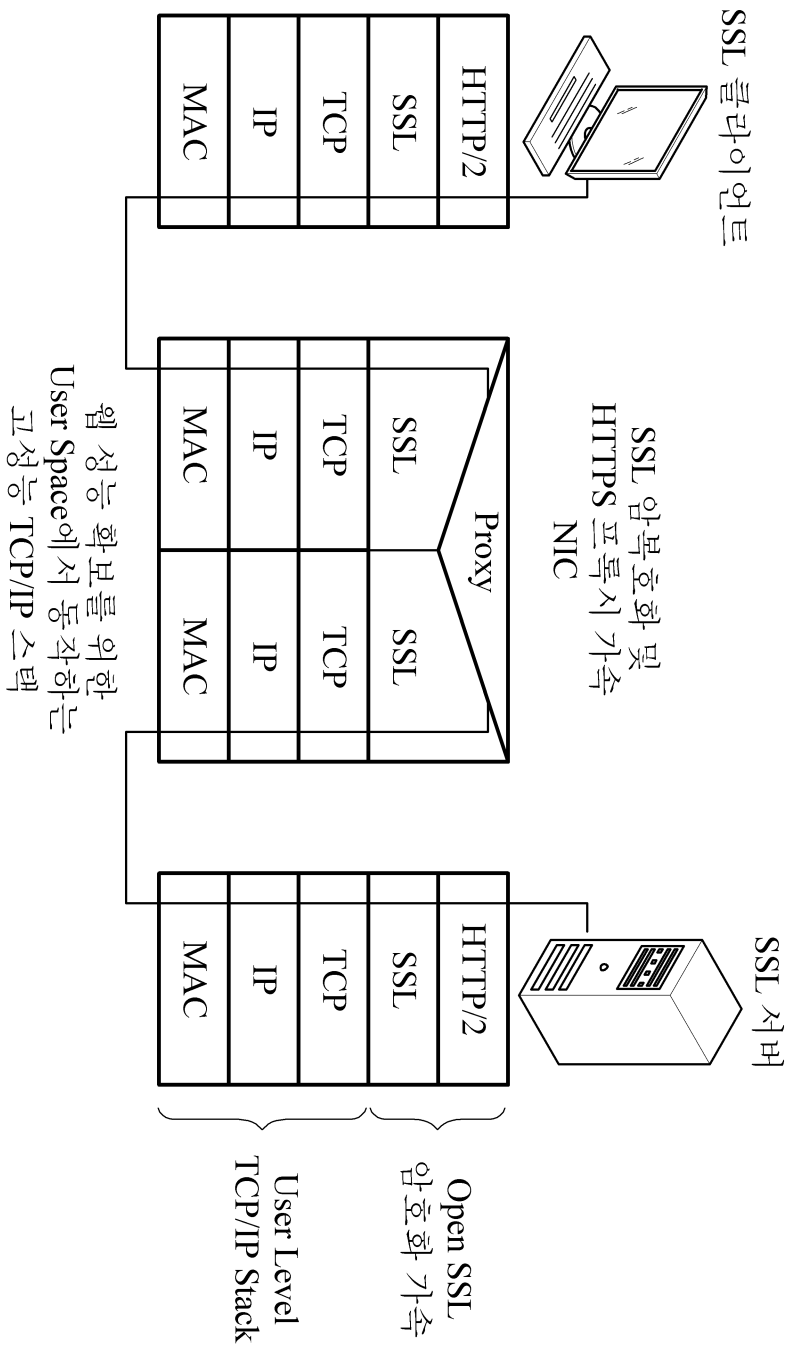
도면7


Receive-Side Scaling (RSS)
Parsed receive packet
RSS hash
32
packet Descriptor
7LS bits
7
Redirection Table 128 x 4
4
4
RSS output index
0
RSS Disable or (RSS & not decodable)
(a)
Data Center Bridging (DCB)
Packet Plane TC Arbiter
Descriptor Plane TC Arbiter
Queues Arbiters one per TC
BCN Rate-Scheduler
Traffic Class 0
PB 0
Round-Robin
DQ 0
DQ 1
DQ 31
Weighted Strict Priority
Descriptor Fetch Arbiter
Traffic Class 7
PB 7
Round-Robin
DQ 120
DQ 121
DQ 127
MAC
Flow Control per TC Manageability packets
Packet Buffers
Data read request
Data
Descriptor Queues
(b)

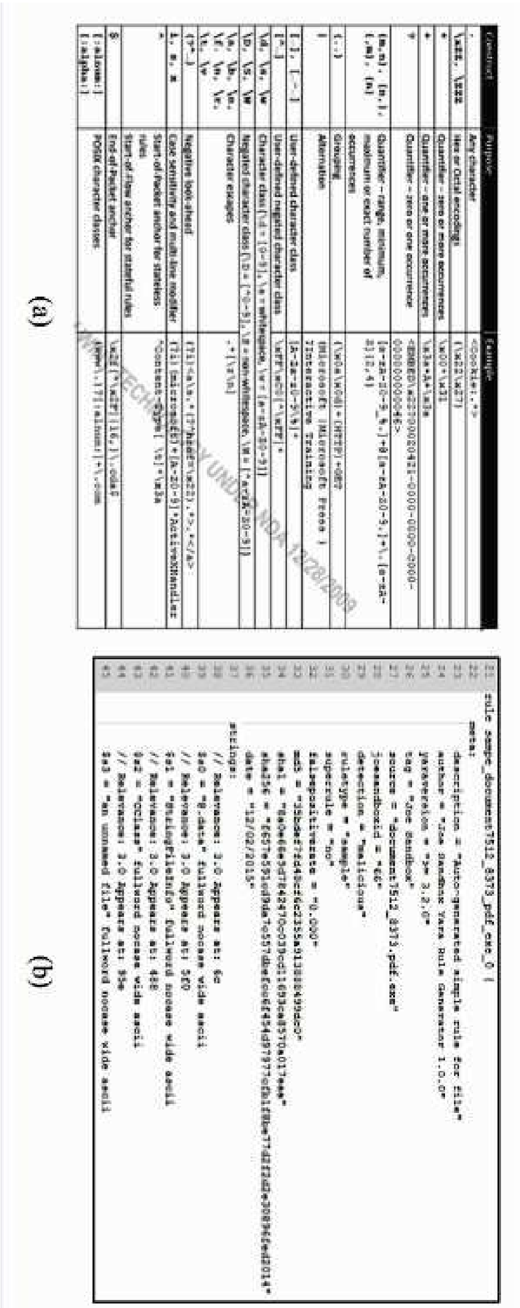
도면8


2
네트워크 보안 및 정보보호 어플리케이션 서버
NUMA
RSS
DPDK
Shared L3 Cache
(25MB)
DDR3 Controller
PCIe G3 Controller
Quick Path
CPU 0
CPU 1
1
10
12
14
멀티 코어
프로세서
범용 네트워크
컨트롤러
PCIe
8x
Pkts
네트워크 보안
어플라이언스
10 GbE 8 포트 수용

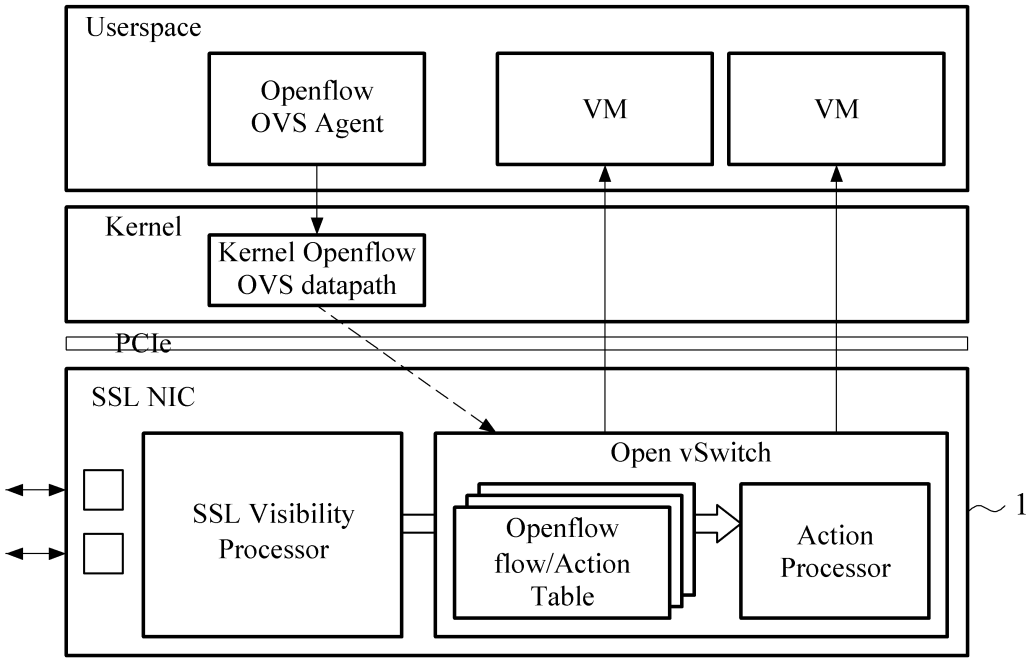
도면9


SSL 클라이언트
HTTP/2
SSL
TCP
IP
MAC
SSL 암복호화 및
HTTPS 프록시 가속
NIC
Proxy
SSL
TCP
IP
MAC
웹 성능 확보를 위한
User Space에서 동작하는
고성능 TCP/IP 스택
SSL 서버
Open SSL
암호화 가속
User Level
TCP/IP Stack

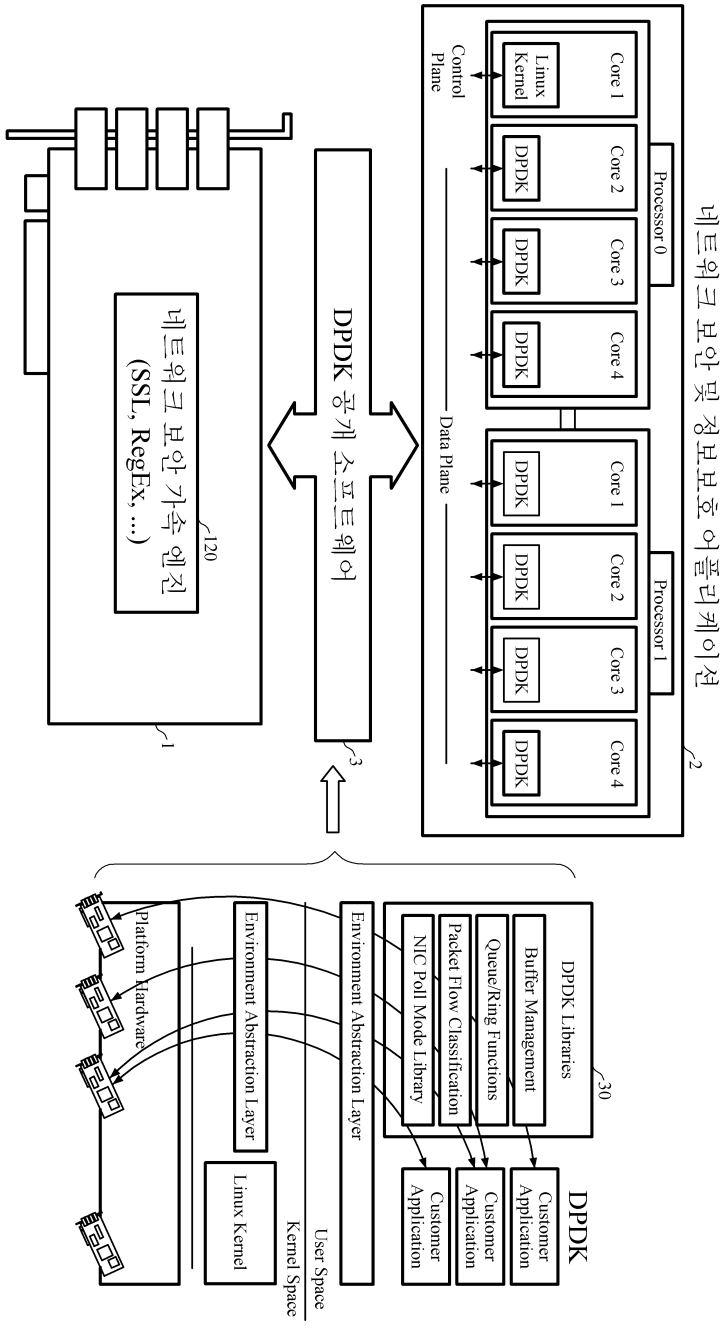
도면10



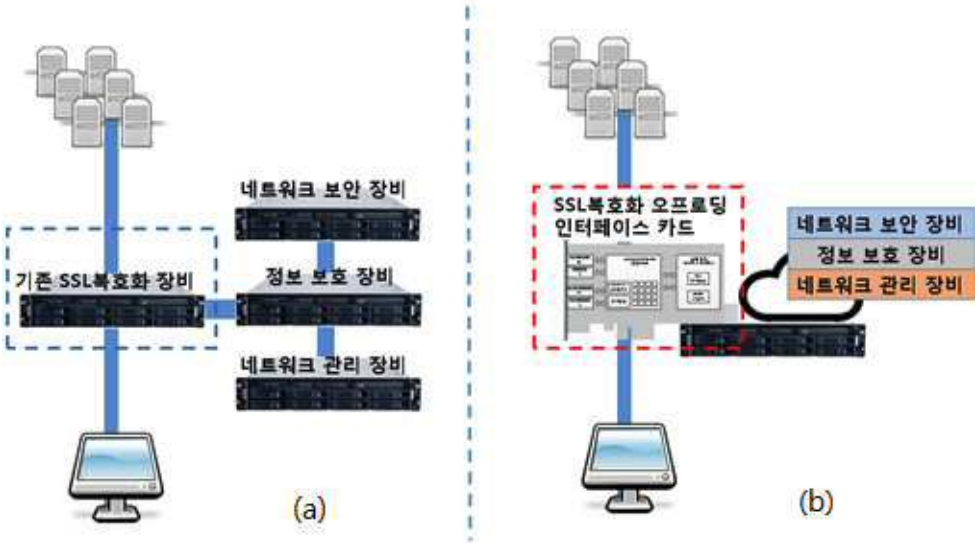
도면11


Userspace
Openflow
OVS Agent
VM
VM
Kernel
Kernel Openflow
OVS datapath
PCIe
SSL NIC
SSL Visibility
Processor
Open vSwitch
Openflow
flow/Action
Table
Action
Processor
1

도면12


네트워크 보안 및 정보보호 어플리케이션
Processor 0
Processor 1
Core 1
Core 2
Core 3
Core 4
Linux Kernel
DPDK
Control Plane
Data Plane
2
DPDK 공개 소프트웨어
3
네트워크 보안 가속 엔진
(SSL, RegEx, ...)
120
1
DPDK
DPDK Libraries
30
Buffer Management
Queue/Ring Functions
Packet Flow Classification
NIC Poll Mode Library
Environment Abstraction Layer
Customer Application
User Space
Kernel Space
Linux Kernel
Platform Hardware

도면13


네트워크 보안 장비
기존 SSL복호화 장비
정보 보호 장비
네트워크 관리 장비
(a)
SSL복호화 오프로딩
인터페이스 카드
네트워크 보안 장비
정보 보호 장비
네트워크 관리 장비
(b)