



White Paper

Network Functions Platform for App Delivery

AVX 시리즈 네트워크 기능 플랫폼

With foreword by:

*Brad Casemore, Research Director, Datacenter Networks
IDC*

머리말 : Brad Casemore, IDC	3
개요	4
네트워크 기능 플랫폼(Network Functions Platform)이란?	6
NFV 와 애플리케이션 딜리버리	6
NFV 전환을 위한 간편한 경로	9

머리말



SDN (Software-Defined Networking)은 클라우드 시대의 요구사항인 민첩성과 밀접하게 부합되는 아키텍처로 지난 10 여 년 동안 발전해 왔습니다. 그리고 얼마 지나지 않아 네트워크 기능 가상화 (NFV) 개념이 부상했습니다. NFV 는 통신서비스 업체 (Comm SP)에 의해 발전되어 왔으며 유럽 전기 통신 표준 협회 (European Telecommunications Standards Institute, ETSI)의 후원으로 공식적으로 정의되었습니다.

NFV 가 통신 서비스 제공 업체를 위해, 또 이들에 의해 설립된 ETSI 에 의해 공식화 되었지만, NFV 가 추구하는 많은 목표는 일반 기업에도 똑같이 적용될 수 있습니다. NFV 는 표준 서버 하드웨어 위에서 실행되는 가상 네트워크 기능(Virtual Network Function)을 통해 운영과 네트워크의 민첩성 향상, Opex 및 Capex 절감, 시장 요구 사항의 변화에 따른 새로운 서비스의 신속한 적용을 가능하게 하고자 했습니다. 이러한 목표는 서비스 사업자에게만 중요한 것이 아니라, 디지털 전환을 꾀하고 있는 많은 기업들 또한 큰 관심을 가지는 분야입니다.

"엔터프라이즈 NFV"라는 용어가 등장했지만 여전히 대부분의 기업 IT 부서는 가상 네트워크 기능 (VNF) 도입의 초기 단계에 머물러 있으며, 완전한 NFV 프레임 워크 내에서 자동화되고 통합 된 VNF 를 본격적으로 채택하고 있지는 않습니다. 예를 들어, IDC 시장 조사에 따르면 2016 년에 기업에 판매된 전체 ADC 매출 중에서 소프트웨어/가상 폼팩터 (vADC)가 차지한 비중은 전체 매출의 19% 미만에 불과 합니다. 실제 기업에서는 어플라이언스로 판매되는 ADC 가 여전히 우세 합니다. 다른 네트워크 및 보안 서비스에서의 사정도 ADC vs vADC 와 크게 다르지 않습니다.

그러나 VNF 채택이 상대적으로 낮은 이유가 NFV 의 원칙과 실체에 관한 기업의 관심이 부족한 때문은 아닙니다. 오히려 IDC 가 만나본 여러 기업들의 반응과 IDC 실제 조사 결과에 따르면 SDN 또는 네트워크 자동화를 추진하거나 도입하려는 기업의 경우, 특히 가상 네트워크 및 보안 서비스를 채택하려는 기업이 늘어나고 있습니다. 그 이유는 기업들이 서비스의 신속한 적용, 네트워크 민첩성 확보, 운영 효율성 향상 그리고 설비 투자와 운영 비용을 낮추고자 하기 때문입니다.

하지만 기업 IT 부서에서 NFV 를 실행하려고 하면 여러 가지 난관에 봉착하게 됩니다. 그 중 하나가 IT 부서 내 여러 팀간의 역할과 책임에 대한 혼란과 심지어 충돌입니다. 실제로 범용 서버에서 실행되는 네트워크와 보안 VNF 가 도입되면 네트워크, 서버, 가상화 및 보안을 담당하는 IT 팀간에 기존에 확립되어 있던 경계선이 흐려질 수 있습니다. 또 다른 문제점은 네트워크 가상화와 같은 영역에서 필요한 기술력의 부족, 표준 서버에서 가상화 된 네트워크 및 보안 서비스를 채택할 때 발생할 수 있는 잠재적인 성능 저하에 대한 우려입니다.

네트워크 기능 플랫폼(Network Function Platform)은 이러한 맥락 속에서 발전했습니다. 이는 기업의 IT 부서에서 NFV 를 구축할 때 저항이 가장 적은 경로를 제공하려는 노력의 산물이기도 합니다. 이 접근 방식은 가상화 된 네트워크 및 보안 서비스 기술에 대한 전반적인 활용 사례에 대한 의구심 뿐만 아니라 운영상에 발생하는 마찰, 기술 격차 그리고 만족스러운 성능에 대한 우려를 해결하기 위한 것입니다.

Brad Casemore, Research Director,
Datacenter Networks
IDC

개요

최근에 네트워크 기능 플랫폼 (Network Functions Platforms)이라고 하는 새로운 클래스의 제품이 IT 업계에서 널리 다루어지고 있습니다. 이 새로운 이름은 NFV (Network Functions Virtualization)와 관련이 있지만, 그것이 전부는 아닙니다. 네트워크 기능 플랫폼에 대해 자세히 살펴보면 이 새로운 솔루션 카테고리가 기업 IT 관리자를 위해 어떤 일을 할 수 있는지 보다 분명해 질 뿐만 아니라, 애플리케이션 딜리버리에 활용할 수 강력한 새로운 방법이 될 수 있다는 것을 알 수 있을 것입니다.

우선, 기업의 NFV 도입과 관련하여 먼저 현재 NFV 환경을 이해하는 것이 중요합니다.

- 최근의 시장 조사 및 분석 보고서에 따르면, 업무 네트워크에서 NFV 를 구축한 기업이 아직 소수이긴 하지만, 전체 기업의 절반 이상이 현재 NFV 전략 및 공급 업체에 대한 분석을 하고 있습니다.
- NFV 를 고려하는 핵심 이유는 **1) 신속한 서비스 제공 2) IT 인프라 활용에 있어 민첩성과 효율성을 높이기 위한 것**입니다. 또한 예상되는 CAPEX 및 OPEX 의 감소 또한 중요한 검토 배경입니다.
- NFV 에 관한 논의가 빠르고 광범위하게 진행되어 가면서 여러 가지 걱정도 함께 커지고 있습니다. **1) 서버, 가상화, 네트워킹 및 보안 팀 간의 전통적 역할 붕괴 및 갈등 2) 신기술에 대한 기술력 부족 3) 현재의 NFV 솔루션의 미성숙 4) ROI 를 명확하게 정의하기 어렵고 5) 엔터프라이즈 급 성능 및 보안에 대한 우려**

기업은 IT 요구 사항을 지원하기 위하여 점점 더 클라우드화 되고 소프트웨어 중심적인 방식으로 움직이고 있기 때문에 NFV 에 대한 관심이 높습니다. Network Functions Platform 은 네트워킹 및 보안 어플라이언스 (VAs) 와 가상 네트워크 기능 (VNF)을 실행하기 위한 목적으로 설계된 가상화 된 하드웨어 플랫폼입니다. 기업이 NFV 도입시 겪게 될 여러 가지 문제점을 네트워크 기능 플랫폼이 해결해 줄 것입니다.

네트워크 기능 플랫폼(Network Functions Platform)이란?

네트워크 기능 플랫폼을 네트워크와 보안 서비스를 위한 강력한 가상화 서버라고 생각하십시오. 네트워크 및 보안 작업의 부하(예 : ADC, WAF 및 DDoS)는 응용 프로그램의 부하에 비해 훨씬 CPU 집약적입니다. 네트워크 기능 플랫폼은 이러한 특징을 가진 가상 네트워크 및 보안 서비스를 위해 특별히 설계되어 확장성 있는 성능과 보장 된 성능을 제공합니다.

또한 네트워크 기능 플랫폼은 서버, 가상화 및 네트워크 구성에 수반되는 복잡한 작업을 추상화, 자동화함으로써 IT 조직간의 혼란과 기술 부족 문제를 완화하도록 설계되었습니다. 이제 NFV 도입시 걸림돌이 되는 3 가지 요소를 살펴보고 네트워크 기능 플랫폼이 이들을 어떻게 해결하는지 살펴 보겠습니다.

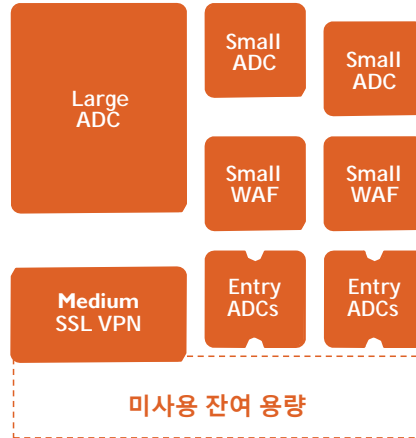
Network Functions Platform

다양한 크기의 인스턴스

다양한 크기의
VAs, VNFs 를 4~
32 개까지 혼합하여
구성가능

사용량에 따른 지불방식

업무 요구량에 따라
Vas 와 VNFs 를
필요한 만큼만 구매



다양한 네트워크 기능

ADC, WAF, SSL
VPN, DDoS, NGFW 등
Array 및 3rd party
vendors 의 기능

관리의 자동화

RESTful APIs 를 이용한
NMS 및 클라우드 관리
시스템과 연동

간편한 구성작업

가상 어플라이언스
하드웨어 리소스를
자동으로 할당하여
복잡성 제거

하이퍼 바이저 관리



성능 보장

VA, VNF 별 전용
CPU, SSL, RAM 및 I
/ O 할당을 통해
성능 보장

- **조직간 갈등** - 네트워킹 팀은 네트워킹 분야에서는 핵심 역량을 갖추고 있지만 대개 서버나 가상화 팀과 별도로 운영되고 있습니다. NFV 를 도입하게 되면 여러 영역의 운영에 영향을 미치기 때문에 결과적으로 조직간의 역할/책임 문제 등으로 혼란에 빠질 위험이 있습니다.

네트워크 기능 플랫폼은 네트워킹 팀이 서버나 가상화 팀의 도움 없이도 구입 및 구축 할 수 있는 어플라이언스입니다. 이 플랫폼은 이미 NFV 를 위한 전용 목적으로 설계되었기 때문에 복잡한 가상화 구성이 자동화 되어 있기 때문에 서버 또는 가상화 팀에 도움을 요청할 필요가 없습니다.

- **기술력 부족** - 앞서 언급했듯이 NFV 는 새로운 기술들이 집합되어 있으며, 이들 중 일부는 네트워크 팀의 영역을 넘어선 지식 (그리고 경우에 따라 서버 및 가상화 팀이 보유하지 않은 기술일 수도 있음) 이기도 합니다. 여기에는 서버 구성정보 선택, 자원 할당, 서비스 체인에 이르기까지 모든 것이 포함됩니다. 이러한 지식이 없으면 NFV 시도는 결국 실패하게 됩니다.

서버 사양, 하이퍼 바이저 관리, CPU 고정, NUMA 경계 설정, SR-IOV, 드라이버, 물리적 및 가상 포트 매핑 및 기타 여러 요소가 네트워크 기능 플랫폼에 의해 완전 자동화되고 추상화됩니다. 네트워킹 팀이 해야 할 일은 단지 원하는 기능과 적절한 크기의 인스턴스를 선택하는 것입니다.

또한 네트워크 기능 플랫폼에서 제공하는 직관적인 WebUI 관리 시스템을 통해 VA 와 VNF 간의 서비스 흐름을 단순화 할 수 있습니다 (예 : 하나 이상의 ADC 인스턴스가 동일한 네트워크 기능 플랫폼에 구축 된 여러 WAF 인스턴스로 트래픽을 로드 밸런싱) - 전문 기술이나 서버 및 가상화 팀의 도움을 받지 않아도 됩니다. 네트워크 기능 플랫폼을 사용하면 네트워킹 팀과 비즈니스가 최소한의 운영 또는 조직으로 단기간에 소프트웨어 중심으로 변화할 수 있습니다.

- **성능 및 SLAs** – 기업용 애플리케이션의 특징은 비즈니스의 핵심이면서 대용량 트래픽, 복잡한 구성과 최종 사용자 환경에 대한 엄격한 요구 사항이 있습니다. NFV 가 서비스를 적용하는 데 필요한 시간을 줄이거나 IT 인프라를 보다 민첩하고 효율적으로 사용할 수 있는 등 여러 가지 장점을 제공하지만, 애플리케이션이 오프라인이 되거나 성능이 떨어지는 등의 상황이 발생한다면 기업이 이를 수용할 수는 없을 것입니다.

범용 가상화 서버는 네트워킹 및 보안 작업보다는 일반 업무용 프로그램 작업 부하에 적합하게 설계되었습니다. 따라서 범용 하드웨어, 하이퍼 바이저 오버 헤드, VM 간 경쟁 및 가상 스위치등이 모두 엔터프라이즈 응용프로그램이 SLA 를 충족하고 유지 관리하는데 필요한 성능에 장애 요인이 되고 있습니다.

이와는 반대로 네트워크 기능 플랫폼은 하드웨어 기반 네트워킹 및 보안 어플라이언스와 동등한 VA 및 VNF 성능을 제공하며 플랫폼에 설치 된 각 VA/VNF 에 대해 보장 된 성능을 제공 할 수 있습니다.

네트워크 기능 플랫폼은 네트워킹 및 보안용으로 특수 제작 된 시스템 아키텍처를 통해 하이퍼 바이저 관리용 리소스가 VAs 나 VNF 에 영향을 미치거나 영향을 받지 않도록 명확하게 분리됩니다. 또한 각 VA 및 VNF 에는 각기 전용 리소스 (예 : CPU 코어, 하드웨어 가속 SSL, 메모리, 가상 포트 및 물리적 인터페이스)가 할당됩니다. 그 결과 네트워크 기능 플랫폼은 클라우드와 가상화가 제공하는 민첩성과 전용 하드웨어 어플라이언스의 장점인 보장된 성능을 동시에 제공합니다.

NFV 와 애플리케이션 딜리버리

NFV 와 관련된 중요한 관심사는 입증 가능한 ROI 를 제공해야 합니다. NFV 도입을 위한 비즈니스 사례를 구축하는 가장 좋은 방법은 먼저 네트워킹 요구 사항을 즉각적으로 해결할 수 있는 간편하고 독립적인 솔루션을 찾는 것입니다. 이와 동시에 NFV 구현을 위한 토대와 마이그레이션 경로를 마련한 것입니다.

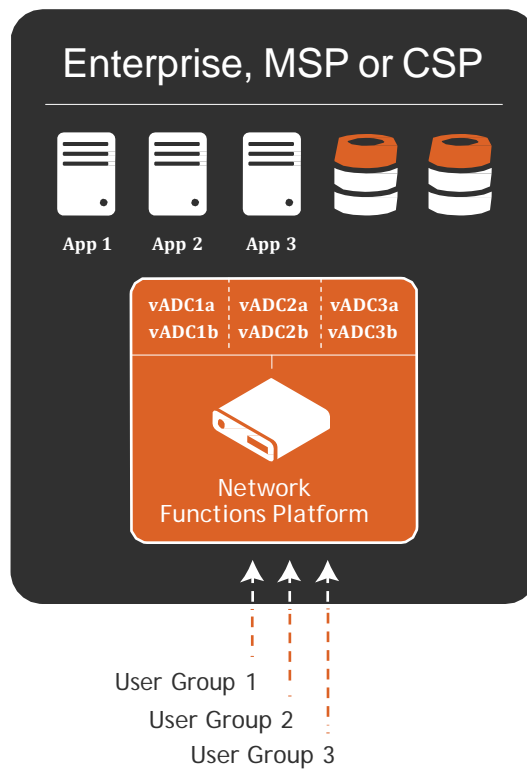
이런 측면에서 보낸 애플리케이션 딜리버리 (고급 로드 밸런싱, Layer-4/7 서비스 및 Layer-7 보안)는 네트워크 기능 플랫폼이 애플리케이션을 빠르고, 가용성 있게 유지하고 보안을 유지하면서 동시에 개선을 제공하는 새로운 구축 모델을 제공 할 수 있는 영역입니다. 기존의 로드 밸런싱 접근 방식과 비교하면 민첩성, 효율성 그리고 경제성을 제공합니다. 적용 가능 분야를 보면 먼저 네트워크 기능 플랫폼을 ADC 멀티 테넌시 및 콘솔리데이션을 지원하는 수단으로 사용합니다. 둘째, Network Functions Platform 을 사용하여 복잡한 애플리케이션 제공 및 보안 구성을 대해 애플리케이션 SLA 를 보장하도록 구성하는 것입니다.

■ ADC 멀티테넌시와 콘솔리데이션

많은 대기업 및 서비스 제공 업체 IDC 에는 많은 수의 전용 ADC 또는 로드 밸런서가 있습니다. 특정 부서, 특정 업무 또는 특정 고객만을 위해 여러 쌍의 ADC 가 할당되는 것은 드문 일이 아닙니다. 이는 각 사업체 또는 업무가 각기 독립적으로 운영되어 다른 업무로 인해 방해 받지 않고 성능을 유지해야 한다는 요구 때문에 발생하는 현상입니다.

그런데 이러한 접근 방식에서는 하드웨어 어플라이언스가 고정적이고 유연하지 못할 뿐만 아니라 비싼 하드웨어 도입비용과 공간, 전력 및 냉각등의 OPEX 비용도 문제입니다. 일부 ADC 공급 업체에서 자신들도 멀티 테넌시를 지원한다고 주장하지만 ADC 인스턴스의 성능을 실제로 독립적으로 분리하거나 보장하는 방식으로 멀티 테넌시를 지원하는 업체는 없습니다.

반면, 네트워크 기능 플랫폼은 진정한 격리와 보장된 성능을 모두 갖춘 ADC 멀티 테넌시를 지원합니다. 각 가상 ADC 인스턴스는 보장된 성능을 제공하는 전용 어플라이언스와 대등한 성능을 제공하기 위하여 각 VM 별로 CPU, SSL, 메모리 및 I/O 리소스를 전용으로 할당하여 독립적으로 운영됩니다. 보안, 가용성 또는 성능의 희생 없이 CAPEX 와 OPEX 를 모두 줄일 수 있습니다.



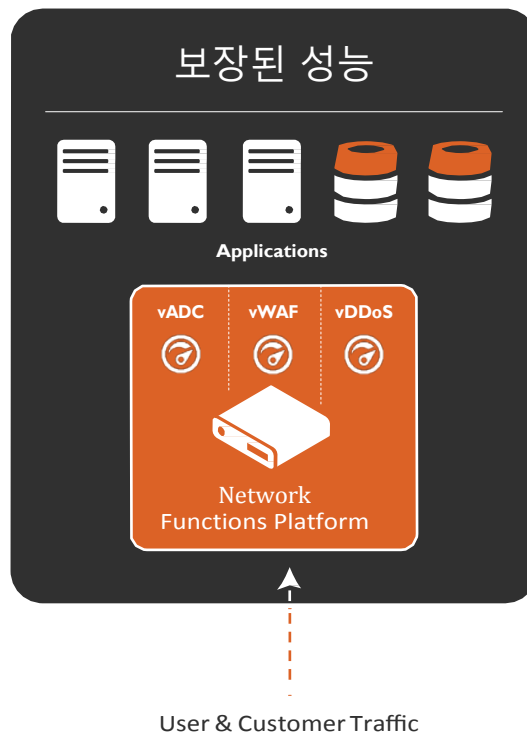
또한 네트워크 운영 팀은 온 디맨드 L4/7 서비스를 원격으로 프로비저닝하고 필요에 따라 확장하거나 축소하여 다양한 애플리케이션, 부서의 변화하는 요구 사항에 맞게 리소스를 재사용 할 수 있는 등 유연성 측면에서 엄청난 이득을 얻습니다. 또한 클라우드 관리 시스템과 통합하여 자동화 할 수 있습니다.

■ 애플리케이션 딜리버리 및 보안 : ADC 서비스의 보장된 성능

애플리케이션 딜리버리는 지난 15 년 동안 상당히 발전했습니다. 초기의 로드 밸런서는 고 가용성을 제공하기 위한 용도였지만 오늘날의 ADC 는 가속 및 고급 보안을 비롯한 여러 가지 기능을 추가로 지원합니다. 예를 들어 로드 밸런싱(ADC)과 웹 애플리케이션 방화벽 (WAF)이 같은 하드웨어 어플라이언스에 함께 설치됩니다.

문서상으로만 보면 이러한 솔루션이 매력적으로 보이지만, 실제로 이들 ADC 공급 업체들은 여기에 대한 언급을 자제하고 있습니다. 이러한 애플리케이션 딜리버리 및 보안 기능은 각각 CPU 중심적인 작업입니다. 다른 말로 하면, 각 기능이 제대로 성능을 내기 위해서는 각 기능이 기기 전체의 리소스를 사용해야 할 수도 있습니다. 따라서 단일 통합 어플라이언스에서 이들을 동시에 활성화하면 일반적으로 성능과 애플리케이션 SLA 가 크게 저하됩니다.

이와는 대조적으로 네트워크 기능 플랫폼은 연산 중심의 고급 애플리케이션 딜리버리 및 하드웨어 서비스와 같은 고성능 보안 서비스를 지원합니다. 어레이 또는 타 벤더에서 제공하는 ADC, WAF 및 DDoS 와 같은 서비스는 각각 완전히 독립적인 VA 또는 VNF 인스턴스로 실행되며, 따라서 각각은 전용으로 할당 된 CPU, SSL, 메모리 및 I / O 리소스를 사용합니다.



자사의 여러 기능으로 수직 통합 된 ADC 를 공급하는 업체들이 안고 있는 공통적인 비밀은 광범위한 제품 포트폴리오를 유지하지만 일반적으로 한 두 가지의 핵심 애플리케이션 딜리버리 및 보안 서비스에 있어서만 우위에 있다는 것입니다. 네트워크 기능 플랫폼은 이러한 벤더 종속을 방지하여 다양한 벤더의 우수한 기능과 일관된 애플리케이션 SLA 를 제공하는 진정한 동급 최강의 솔루션을 구축 할 수 있게 합니다.

NFV 전환을 위한 간편한 경로

네트워크 기능 플랫폼은 멀티 테넌시, 보장된 성능, 동급 최강의 기능, 운영 효율성 및 비용 절감과 같은 애플리케이션 딜리버리가 제공하는 이점 이외에도 매우 중요한 다른 이점을 제공합니다. 즉, 보다 포괄적인 기업의 NFV 전환 작업을 위한 간편하고 안전한 경로를 제공합니다.

네트워킹 팀은 보안 팀과 마찬가지로 플랫폼에서 광범위한 서비스를 시험하고 구축할 수 있습니다. 플랫폼에 친숙해 지면 특정 응용 프로그램이나 최종 사용자의 요구 사항을 충족시킬 수 있는 보다 복잡한 서비스 체인이 등장하게 됩니다. 시간이 지나면 관리 프레임 워크와의 연동하여 대형 사설 클라우드 아키텍처 내에서 플랫폼과 기능 프로비저닝을 중앙 집중화하고 조율하며 자동화합니다.

무엇보다 중요한 것은 네트워크 기능 플랫폼 (Network Functions Platforms)을 통해 기업이 자체적으로 NFV를 향한 계획을 수립할 수 있다는 것입니다. 네트워크 기능 플랫폼은 ROI를 달성하고 기존 애플리케이션 딜리버리 문제를 해결하며, 조직의 혼란과 기술 결함과 같은 NFV 문제를 완화함으로써 NFV 전환시 비용을 크게 절감하며 비즈니스 민첩성을 향상시키기 위한 이상적인 출발점을 제공합니다.

Array Networks

네트워크 기능 플랫폼 회사 인 Array Networks 는 보장 된 성능으로 가상 응용 프로그램 제공, 네트워킹 및 보안 기능을 적용하기 위한 목적의 시스템을 개발합니다. Silicon Valley 에 본사가 있는 Array 는 가상화, 클라우드 및 소프트웨어 중심 컴퓨팅 분야의 폭발적인 성장을 활용할 준비가 되어 있습니다. 전 세계 5000 여 고객사에서 입증 된 Array 는 규모의 민첩성을 제공하는 차세대 기술에 대해 선도적인 분석가, 기업, 서비스 제공 업체 및 파트너가 인정한 제품입니다.



문의처 :

www.arraynetwork.co.kr
array-sales@arraynetwork.co.kr