이것만은 알아야 할 네트워크 보안 이야기

Part 3. 방화벽 - 3 (가상화 기술을 통한 방화벽의 진화)

글. 이선응 아이크래프트 수석

이번 시간에는 가상화 기술이 발전하면서 거기에 맞추어 방화벽이 어떻게 발전했는지 알아보자.

가상화 기술의 등장 배경

CPU의 코어(core) 수가 증가하면서, 하나의 CPU에서 동시에 여러 개의 OS를 구동할 수 있는 기술이 발전하였다. 이 기술을 통해 가상 서버의 사용이 활성화되면서, 이 기술을 서버가 아닌 네트워크 장비에도 활용하고 싶은 수요가 생기면서 NFV(Network Function Virtualization, 네트워크 기능 가상화)라는 용어가 등장하였다.

현재 대부분의 네트워크 장비, 예를 들면 라우터, 스위치, 방화벽 등은 서버 형태가 아닌 별도의 전용 장비로 공급된다. 하지만 이런 장비들도 최초에는 일반적인 서버에 프로그램방식으로 설치되어 사용되기 시작했다. 지난 호에서 소개한 1세대 방화벽의 시초인 체크포인트(checkpoint)의 경우에도 처음에는 H/W가 아니라 S/W로 출시되었다. 즉, 방화벽을 설치하기 위해서 일반적인 서버를 구매하여 방화벽 소프트웨어를 설치하고, 서버 뒤에 네트워크 케이블을 연결하여 동작시켰다. 2000년 초중반까지도 이런 방식처럼 서버 형태로 공급되어 별문제 없이 사용되었다. 아주 높은 성능을 요구하지 않는 환경에서는 범용 서버의 CPU 성능으로도 웬만한 트래픽은 문제없이 처리할 수 있었다.
하지만 점점 처리해야 할 트래픽이 증가하면서 범용 서버의 성능으로는 한계에 다다르게 되었다. 이제 범용 서버가 아닌 전용 장비가 필요한 시기가 된 것이다. 이때 등장한 것이 넷스크린(Netscreen)이라는 방화벽이다. 이 회사의 방화벽은 기존 S/W 방식으로 제품을 팔지 않고 전용 장비에 전용 OS를 설치하여, 그 당시에는 획기적인 성능인 2Gbps

그림 1. 최초의 Giga 급 방화벽(Netscreen 1000)과 동일 성능의 최신 방화벽

의 처리 성능을 내는 장비까지 출시하였다. [그림 1]과 같이 대략 13U(56cm)로 랙의 거의 절반을 차지하는 크기에 무게는 23kg이었다. 범용 CPU가 아니고 전용 ASIC 칩(주문형 반도체, 특정한 기능을 가속해서 처리할 수 있도록 개발된 칩)을 직접 개발하여 적용하고 유닉스를 커널 컴파일(제작자의 의도에 따라 OS를 최적화시키는 작업)하고, 전용 OS를 개발하여 적용하였기 때문에, 기존 범용 서버에서 나오는 성능의 대략 10배 이상의 성능을 달성할 수 있었다.

가상화 기술의 정의

그럼 먼저 서버 가상화 기술에 대해 알아보자. 가상화 기술은 물리적으로 독립된 서버에 여러 개의 가상 서버를 동시에 운영할 수 있는 기술이다. [그림 2]의 왼쪽 서버처럼 제일 하단에 검은색의 CPU, 메모리, 저장장치, 랜카드로 이루어진 서버 하드웨어가 존재하고, 그 상단에 윈도우 혹은 리눅스, 유닉스 등의 운영체제가 설치된다. 이렇게 운영체제가 설치되면, 사용자가 원하는 Web, DNS, Mail 등의 응용프로그램이 설치되어 독립된 서버로 동작하게 된다.
그런데 [그림 2]의 오른쪽 서버와 같이 동일한 하드웨어에 OS 대신에 VMware 같은 하이퍼바이저(Hypervisor)가 설치되면 CPU에 있는 각각의 코어(Core)를 독립된 하나의 가상 CPU로 인식하여, 하나의 가상 서버를 구성할 수 있도록 해준다. 또한 메모리, 하드디스크 등도 사용자가 설정하는 용량만큼 분할하여 각각의 가상 서버에 독립적으로 할당시켜 물리적으로 한 개의 메모리와 하드디스크가 가상 서버 개수만큼 존재하는 것처럼 동작하게 도와준다.

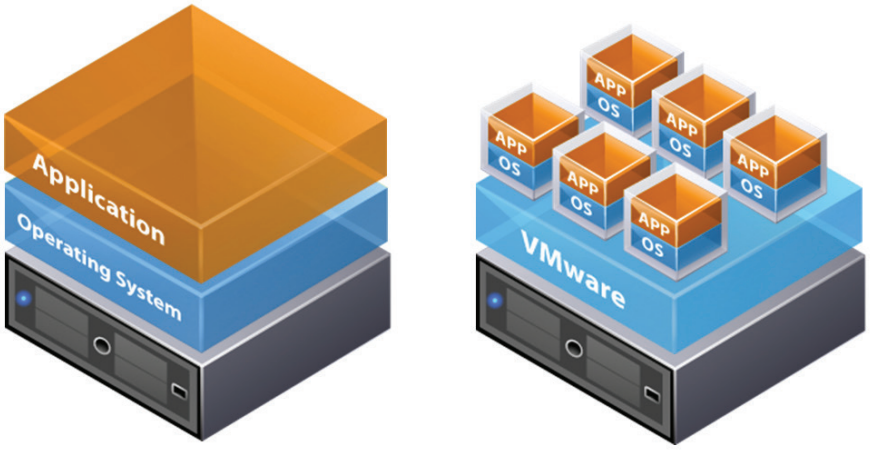

그림 2. 전통적인 서버와 가상화 서버 비교 / 출처 : VMWare

이렇게 생성된 가상 서버를 보통 VM(Virtual Machine)이라고 말한다. 요즘 인텔 서버용 CPU당 코어 수는 모델에 따라 4개에서 28개까지 장착되어 있어 하나의 CPU가 있는 서버에 VM당 2개의 코어를 할당한다고 가정하면 최대 14개의 VM을 작동시킬 수 있다. 물리적으로 한 대의 서버에 14개의 가상 서버를 운영할 수 있다면 가상화를 사용하지 않는 서버만 운영할 경우보다 서버 운영 자원의 절감이 가능하다. 랙에 설치되어 차지하는 공간, 전원 소모량, 발열을 냉각하기 위한 항온항습기 전기 소모량 등 서버 유지비의 획기적인 절감이 가능하므로 많은 조직에서 규모의 차이만 있을 뿐 많은 서버를 가상 서버로 운영하고 있다.
물리적인 자원의 절감뿐만 아니라 서버를 운영하는데 있어서도 많은 편의성이 증대된다. 신규로 OS를 설치할 경우 짧게는 20분에서 1시간 이상의 시간이 소요되었지만, 가상화 기술을 이용하게 되면 VM이 하나의 파일로 만들어지기 때문에, 하이퍼바이저를 통해 동일한 OS에 동일한 소프트웨어가 설치된 VM을 배포하여 3~5분 이내에 원하는 개수만큼 바로 사용할 수 있다. 그리고 VM에 할당하는 CPU, 메모리를 하드웨어 자원에 여유가 있다면 VM에 할당하는 자원을 원하는 만큼 늘이거나 줄일 수도 있고, 저장 공간도 늘일 수 있기에 서비스 접속자의 증가에 유연하게 대응이 가능하다.

VM이 파일 형태로 존재하므로 하드웨어의 공간적 제약도 없다. 특정 서버에 있는 VM들의 사용량이 증가하여 해당 서버의 CPU 사용량이 많아지더라도 가상화 관리프로그램이 자동으로 CPU 자원에 여유가 있는 서버로 VM을 중단 없이 이동시킬 뿐만 아니라 하드웨어의 장애가 발생하더라도 VM을 짧은 시간 내에 다른 서버에서 재가동 시키기 때문에 서버 관리자의 업무량도 획기적으로 줄일 수 있게 되었다.

가상화 기술의 활용

서버 가상화를 운영 중인 조직은 자기도 모르는 사이에 아주 기초적이기는 하지만 NFV 기술을 사용하고 있다고 볼 수 있다. 여러 대의 VM들이 하나의 서버에서 작동하게 되면 같은 서버 내의 VM 간의 통신뿐만 아니라 서버 외부의 다른 서버와도 통신이 필요하다. [그림 3]과 같이 하이퍼바이저 내에는 'vSwitch'라는 가상의 스위치가 존재한다. 물리적인 스위치 대신에 가상의 스위치를 이용하기 때문에 사용 포트 수의 제한이나, 물리적인 케이블의 연결이 필요 없게 된다.

[그림 3]의 왼쪽 그림과 같이 총 4개의 VM이 있고, 각각 vNIC이라는 가상의 네트워크 카드를 통해 vSwitch에 가상으로 연결되어 있다. 이를 통해 오른쪽 3개의 서버 VM이 서로 통신이 가능하게 되어 있다. 제일 왼쪽 VM은 방화벽 프로그램을 구동시켜 방화벽으로 동작 중이다. 서버 VM에 연결된 가상 스위치가 방화벽 VM으로 연결되어 있고, 방화벽 VM은 다시 다른 가상 스위치를 통해 서버 외부로 연결되어 있다. 이렇게 가상으로 연결된 네트워크 구성을 실제 장비로 동일하게 구성하면 오른쪽 그림과 같다. 서버 3대가 하단 스위치에 연결되어 있고, 하단 스위치는 방화벽에 방화벽은 상단 스위치에 연결되어 있어 인터넷 등의 외부 네트워크로 통신이 가능하게 구성할 수 있다.

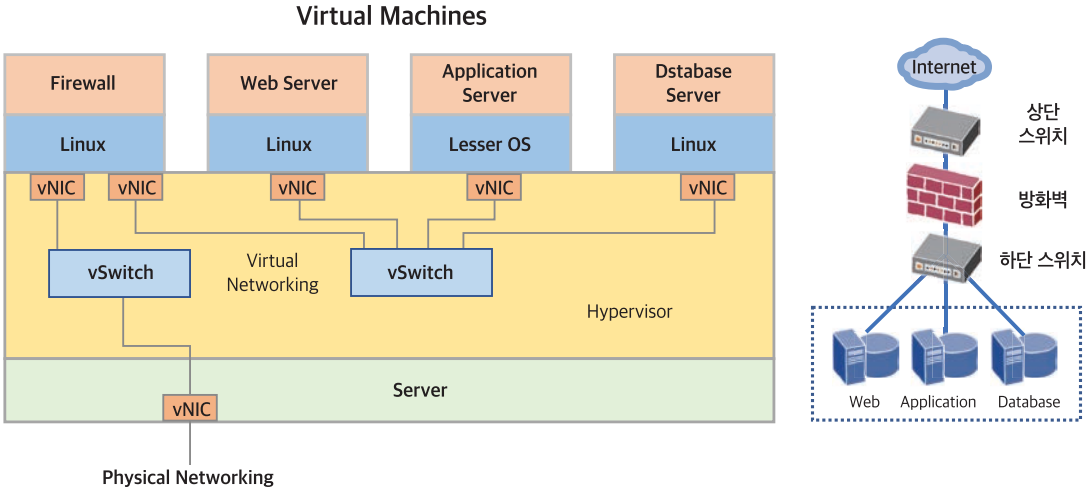

그림 3. 가상 스위치를 통한 네트워크 구성 예 (Virtual vs Real)

서버 3대, 스위치 2대, 방화벽 1대를 구성할 경우, 차지하는 공간, 소비되는 전력량, 발열로 인한 냉각 비용을 고려하면, 총 6대의 장비를 서버 1대로 구성할 수 있게 되어 여러 물리적인 자원의 획기적인 절감이 가능해진다. 그뿐만 아니라, 이렇게 가상으로 구성된 전산 자원이 소프트웨어적인 파일 단위로 존재하기 때문에 쉽게 복제하여, 짧은 시간에 동일하게 구성할 수도 있다. 구성 변경을 할 경우에도 장비가 있는 데이터센터에 직접 가서 장비를 추가로 설치하거나 네트워크 케이블을 연결할 필요 없이 원격에서 관리프로그램을 이용하여 손쉽게 장비를 추가, 삭제하거나 네트워크 연결 수정이 가능하다.

보통 [그림 3]과 같이 VM에 일반적인 웹, DB 같은 서버 프로그램 대신에 방화벽, 라우터, 스위치 프로그램을 동작시켜 가상화된 네트워크 기능을 수행하는 것을 NFV(네트워크 기능 가상화)라고 정의한다. 네트워크 장비공급사인

그림 4. 주니퍼 가상 방화벽 소개 문구vs Real)

시스코, 주니퍼 등의 종합 벤더뿐만 아니라 포티넷, 팔로알토 네트웍스, 파이어아이 등의 보안 전문 벤더까지 실제 장비와 동일한 기능을 수행하는 소프트웨어를 출시 중이다. [그림 4]와 같이 일반적으로 기존에 출시되던 제품명 앞 혹은 뒤에 V 혹은 VM 이라는 이름을 붙여서 소프트웨어로 제품을 판매하고 있다.

가상화 기술을 통한 가상 방화벽

네트워크 장비를 하드웨어 제품으로 공급할 경우에는 하드웨어의 처리 성능에 따라 모델을 구분하여 판매하였으나, 가상화 제품의 경우 소프트웨어만 판매하므로 설치되는 서버에 따라 성능이 결정된다. [그림 5]와 같이 사용하는 하이퍼바이저의 종류 및 VM에 할당되는 코어의 개수와 메모리 크기에 따라 처리 성능의 차이가 보인다. 하이퍼바이저 중에 상용제품으로 VMWare는 가상화시장을 개척했다고 할 수 있을 정도의 오랜 업력과 높은 점유율을 차지하고 있고, 리눅스 기반의 KVM의 경우 높은 성능과 무료로 사용할 수 있는 장점 때문에 고객의 선호도가 높은 하이퍼바이저이다.
하이퍼바이저의 종류, 동작하는 서버의 스펙에 따라 최소 9.5Gbps에서 최대 98Gbps의 성능을 낼 수 있어 고객이 원하는 처리능력에 따라 적절하게 자원을 할당하고, VM 생성 후 사용이 가능하다. 정상적인 경우에는 처리 용량이나 사용 기간에 따라 소프트웨어 라이센스를 구분해서 사용하는 것이 일반적이나, 현재까지는 가상 방화벽의 보급이 초기 단계이기 때문에 특별히 제한을 걸지 않고 사용할 수 있게 하는 벤더도 많이 있는 것으로 알고 있다.

Performance and Capacity[1]	VMware				KVM			
vCPUs	2	5	9	17	2	5	9	17
Memory	4 GB	8 GB	16 GB	32/64 GB	4 GB	8 GB	16 GB	32/64 GB
Firewall throughput, large packet (1514B)	9.5 Gbps	14 Gbps	73 Gbps	81 Gbps	14 Gbps	39 Gbps	68 Gbps	98 Gbps
Firewall throughput, IMIX	2.4 Gbps	4.1 Gbps	17 Gbps	27 Gbps	3.2 Gbps	14 Gbps	16 Gbps	27 Gbps
AES+GCM IPSec VPN throughput (1420B)	2.2 Gbps	4.2 Gbps	12 Gbps	13 Gbps	1.1 Gbps	7 Gbps	10 Gbps	16 Gbps
Application visibility and control[2]	2.4 Gbps	7.2 Gbps	21 Gbps	39 Gbps	3.3 Gbps	10 Gbps	19 Gbps	38 Gbps
IPS recommended signatures	2.3 Gbps	7.1 Gbps	18 Gbps	39 Gbps	3 Gbps	10 Gbps	19 Gbps	36 Gbps
TCP connections per second	55,000	166,250	351,250	537,660	69,000	239,380	360,000	612,660
Maximum concurrent sessions[3]	512,000	2M	4M	12/24M	512,000	1M	1.5M	12/24M

그림 5. 주니퍼 가상 방화벽 하이퍼바이저 및 vCPU 수량별 성능 비교표

방화벽 관리자가 가상 방화벽을 설치할 경우 벤더에서 제공하는 하이퍼바이저별로 VM 이미지 파일을 내려받아서 VM을 시작하면 초기 설치 단계로 통해 운영에 필요한 관리 IP 주소, 계정정보 등의 초기 설정을 하게 된다. 가상 방화벽과 하드웨어 방화벽의 다른 점은 배포 방식밖에 없다. 간혹 하드웨어 내의 특정 부품을 통해 지원되는 기능의 경우 가상장비에서는 해당 부품이 없기에 지원되지 않는 기능이 종종 있기는 하지만, 이런 기능들도 조금씩 가상장비에서 지원이 가능하도록 개선되고 있다.

이러한 가상 방화벽의 경우 일반 기업 단위에서 많은 수의 VM을 사용 중이라면 유용하게 사용할 수 있다. VM을 서비스 종류별로 그룹을 묶어서 방화벽 뒤에 배치하거나, 보안이 필요한 중요 자료(인사, 회계, 제품개발)가 저장된 VM 앞에 별도로 배치하여 사내에서도 접근을 엄격히 제한하는 용도로 사용할 수 있다. 최근에는 클라우드의 사용이 증가하면서 퍼블릭 클라우드(Public Cloud, 공공 클라우드)에서도 이런 가상 방화벽을 사용할 수 있도록 서비스하고 있다.
대표적으로 아마존웹서비스(AWS)의 경우 [그림 6]과 같이 제공되는 VM의 하드웨어 사양에 따라서 시간 단위 혹은 연 단위로 가격을 차등적으로 적용해서 구매 후 사용이 가능하다. 예를 들면 c4.xlarge 등급의 VM에 KVM 하이퍼바

이저를 사용할 경우 대략 8 core, 7.5G 메모리를 제공하므로 39Gbps의 처리 성능 방화벽을 시간당 0.749달러에 사용할 수 있다. 연 단위로 환산하면 소프트웨어 2,280달러와 하드웨어 1,743달러 합해서 4,023달러가 되며, 우리 돈으로 계산하면 대략 483만 원 정도가 필요하다. 하드웨어의 내구 연한을 7년 정도로 잡으면 3,381만 원이 필요하다. 현재 사용되고 있는 하드웨어 방화벽과 비교할 때 성능대비 가격이 합리적으로 보이는가?

vSRX Next Generation Firewall

Switch to annual pricing for savings up to **53%**

Hourly | Annual

EC2 Instance type	Software/hr	EC2/hr	Total/hr
c4.xlarge ★Vendor Recommended	$0.55	$0.199	$0.749
c4.2xlarge	$0.55	$0.398	$0.948
c4.4xlarge	$0.55	$0.796	$1.346
c4.8xlarge	$0.55	$1.591	$2.141
c5.large	$0.55	$0.085	$0.635

vSRX Next Generation Firewall

Switch to annual pricing for savings up to **53%**

Hourly | Annual

EC2 Instance type	Software/yr	EC2/hr	Percent Savings (%)
c4.xlarge ★Vendor Recommended	$2,280.00	$0.199	53%
c4.2xlarge	$2,280.00	$0.398	53%
c4.4xlarge	$2,280.00	$0.796	53%
c4.8xlarge	$2,280.00	$1.591	53%
c5.large	$2,280.00	$0.085	53%

그림 6. 아마존웹서비스에서 제공하는 주니퍼 가상 방화벽 시간당, 연간 가격표

웹을 통해 많은 수의 가입자 혹은 시청자, 고객을 주 대상으로 하는 서비스는 공공 클라우드로 서비스를 하기 위해 전산 자원을 이전하는 조직이 늘고 있다. 단시간 내에 수요가 폭증하거나, 해외에서 접속하는 시청자가 늘어날 경우, 사내 시스템으로 짧은 시간 내에 수십 배에서 수백 배 늘린다는 것은 불가능한 것이다. 더욱이 해외에서 서비스를 증설하는 것은 국내보다도 더 많은 시간이 필요하다.

최근 코로나 19 사태로 학교의 개학이 늦어지면서 온라인수업으로 학기 운영이 대체되었다. 온라인수업을 하기 위해서는 실시간 영상회의 서비스, VOD 서비스 등을 위해 다양한 서버와 네트워크 장비가 필요하다. 학생이 접속하여 사용하는 출석 체크, 채팅 서버, 화상회의 서버, VOD 스트리밍 서버, 영상자료 DB 서버뿐만 아니라 여러 대의 서버의 부하 분산을 위한 L4 스위치, 서비스 포트 이외의 접근 시도를 차단하기 위한 방화벽 등이 필요하다.

클라우드에서는 이런 서비스들을 모두 가상화 기술로 지원하고 있다. 기본적으로 필요한 L4 스위치, 방화벽은 클라우드 업체에서 서비스를 제공하고 있지만, 기본적인 기능만 지원하고 좀 더 다양한 기능이나 고성능을 내기 위해서는 기존의 네트워크 벤더에서 개발한 가상화장비를 사용해야 한다. [그림 7]과 같이 공공 클라우드에서는 여러 벤더에서 제공하는 다양한 종류의 방화벽을 제공하고 있다. 다양한 리뷰나 가격을 참고하거나, 관리자가 기존에 운영하거나 선호하는 벤더의 장비를 선택 후 바로 설치하여 서비스가 가능하다.

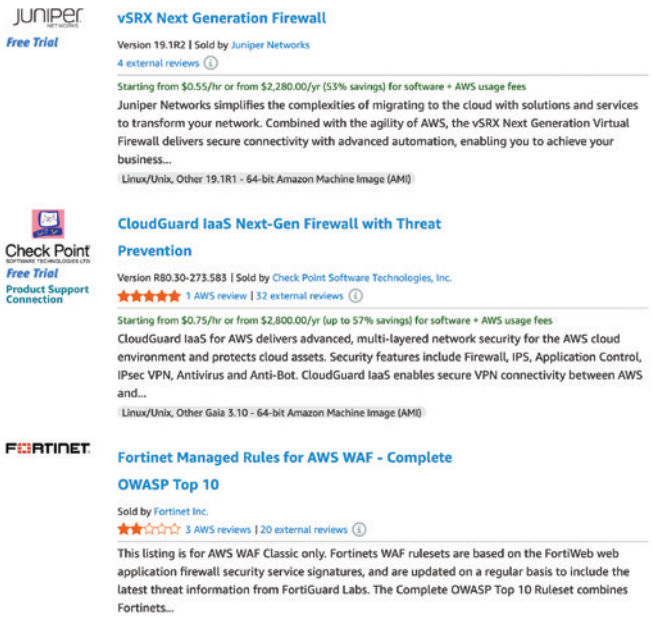

그림 7. 아마존웹서비스 장터(marketplace)에서 제공하는 다양한 가상 방화벽

이러한 가상화 기술은 클라우드 서비스가 활성화되면서 점점 보급이 확대되고 있다. 조직의 모든 전산 자원을 공공 클라우드로 한 번에 옮기는

것이 아니라, 하나의 파일럿 서비스를 선별하여 클라우드로 옮겨서 점진적으로 서비스 품질을 테스트를 진행하고 담당자의 클라우드 운영 경험을 높이는 방향으로 조직의 전산 자원 활용능력을 높이고 있다.

[그림 8]과 같이 사내에는 사설 클라우드를 운영하고 조직 바깥에서는 공공 클라우드를 운영하는 방식으로 진화하고 있다. 조직 내의 중요정보(인사, 재정, 회계, 기획, 고객)를 조직 외부의 공공 클라우드에서 운영하는 것에 대해 거부감이 크다. 중요데이터가 외부, 특히나 해외의 서버에 저장될 경우 데이터 관리에 대한 여러 가지 법적, 심리적, 기술적 문제가 발생할 소지가 있으므로 사내 업무는 사내에 구축한 사설 클라우드를 운영하고, 고객서비스 위주로 공공 클라우드를 운영하는 이원화 방식을 보통 하이브리드 클라우드라고 부른다.

고객 온라인서비스에 필요한 전산 자원을 아주 짧은 시간 내에 신규 구성하고, 서비스 요청이 증가하면 자동으로 전산 자원을 증설하고, 서비스 요청이 줄어들면 전산 자원도 같이 줄어드는 기능, 서비스를 중단할 경우 아주 쉽게 전산 자원을 폐기할 수 있는 기능들은 다양한 이슈로 급변하는 현재의 비즈니스 환경에 최적화되어 있는 기술이라고 할 수 있다.

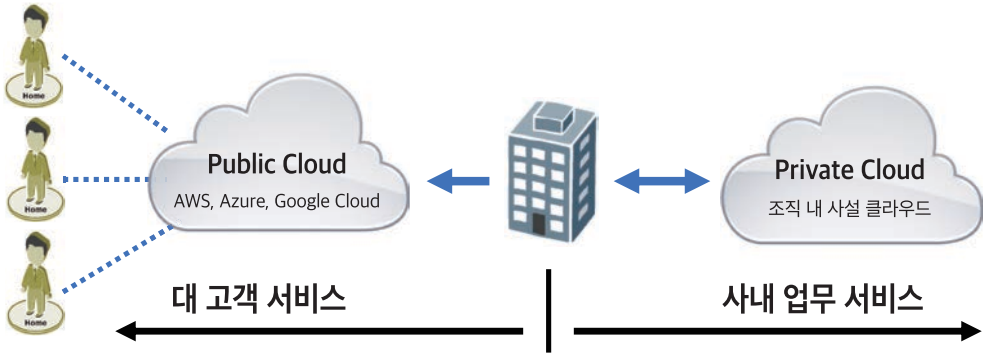

그림 8. 하이브리드(Hybrid) 클라우드 서비스 개념도

가상화 기술의 발전 방향

마지막으로, 가상화 기술의 발전 방향에 대해 소개하고 이번 호를 마치도록 하겠다. 가상화 기술은 하이퍼바이저라는 기능을 통해 발전하였다. 물리적인 서버 위에 하이퍼바이저를 설치한 후 VM 대수를 늘리는 방식으로 서비스 능력을 증가시켰다. 그런데 동일한 조건의 CPU와 메모리를 사용하는 일반 서버와 VM을 비교해 보니 VM의 전반적인 성능이 일반 서버에 비해 낮다는 점이 가상 서버의 가장 큰 약점이었다. 이 문제는 VM을 사용하기 위해서 Guest OS를 반드시 설치해야 하는 조건 때문에 발생한다. 고객에게 직접 서비스를 제공하는 프로그램 입장에서는 VM 내의 Guest OS와 서버의 Host OS 총 2개의 OS를 거쳐야만 CPU, 메모리 등의 자원에 접근할 수 있다. OS를 거칠 때마다 응답시간이 조금씩 늘어나기 때문에 서비스를 받는 고객 입장에서는 서비스가 느려지는 문제가 생긴다. 서비스 제공자 입장에서는 서비스가 느려지지 않게 하기 위해서 VM의 스펙이나 개수를 증가시키는 방식으로 대응할 수밖에 없었다. 이 문제는 VM에서 생기는 오버헤드(Overhead)를 최소화해야 해결 가능하다.

그래서 나온 기술이 Container 기술이다. 하이퍼바이저 대신에 컨테이너 엔진을 이용하여 VM 대신에 컨테이너를 만들어서 내부에 별도의 Guest OS를 설치할 필요 없이 바로 프로그램으로만 구성하여 작동시킬 수 있도록 하였다. 현재 사실상의 컨테이너 표준 기술은 도커(Docker)이다. [그림 9]와 같이 고래 위에 컨테이너를 실어서 운반하는 것처럼 여러 가지 프로그램을 박스화하여 간편하게 사용할 수 있도록 한다는 것을 표현한 이미지이다.
다음페이지 그림과 같이 하아퍼바이저 기술과 비교해 보면 Hypervisor 계층과 Guest OS 계층이 Container Engine으로 대체되었다. 프로그램과 동작에 필요한 라이브러리, 바이너리 파일을 묶어서 박스화 시켜 하나의 파일로 만든

다음 VM과 동일하게 도커 엔진에서 이 파일을 구동하는 방식으로 동작한다. VM과 비교해 보면 OS가 하나 없어진 것밖에 없지만 응답속도는 획기적으로 개선되었다. 그뿐만 아니라 VM의 크기는 Guest OS를 포함하기에 대략 수백 메가에서 수십 기가까지 용량이 컸지만, 컨테이너 파일의 수십 메가에서 1~200메가까지 크기가 작아져서 저장 배포가 더 쉬어졌다. 부팅속도에서도 VM의 경우 1~3분 정도가 걸렸다면 컨테이너는 OS가 없어 수초에서 30초 이내로 부팅이 완료되어 사용 가능하기 때문에 클라우드 환경에서 신속하게 서비스용량을 증가시켜야 할 경우 유용하게 사용 가능한 장점이 있다.

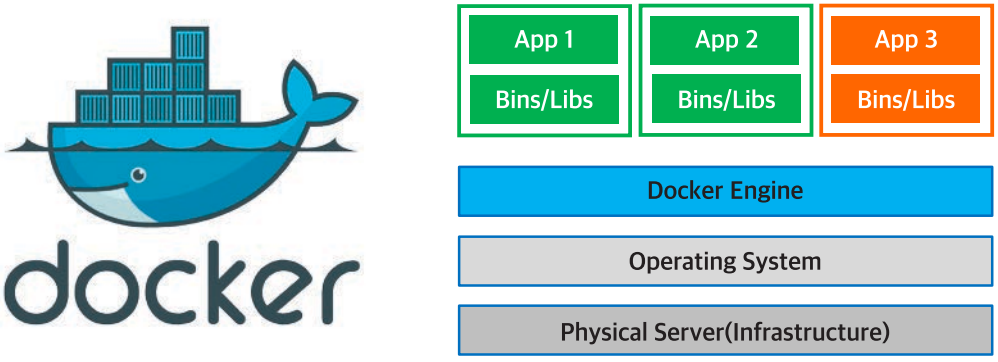

그림 9. 컨테이너 기술의 사실상 표준이 된 도커(Docker)

마지막으로 [그림 10]은 PNF, VNF, CNF를 비교하여 표시하였다. 기존의 물리적인 네트워크 장비는 PNF(Physical Network Function), 가상화된 네트워크 장비를 VNF(Virtual Network Function), 컨테이너 기반 네트워크 장비를 CNF(Container Network Function)이라고 표현하였다.

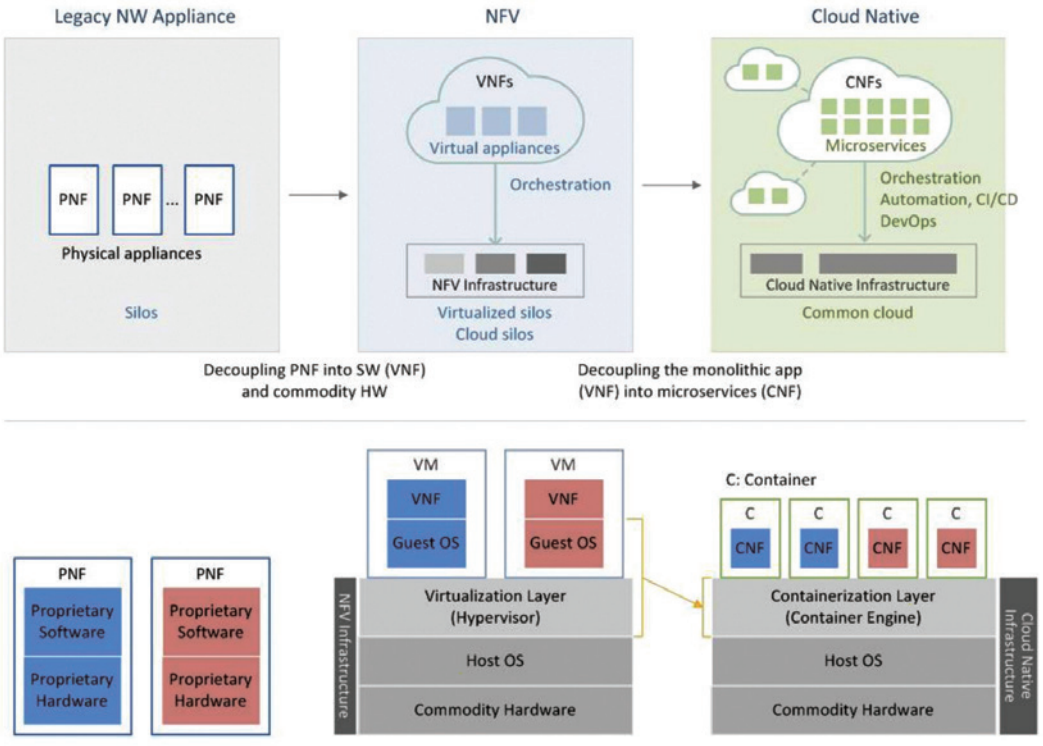

그림 10. PNF, NFV, CNF 비교 / 출처 : 넷매니아즈

네트워크 장비의 시작은 PNF로 시작되어 물리적인 전용 장비로 동작하는, 대략 1990~2005년까지의 기술이라고 하면, 서버의 멀티코어 기술과 하이퍼바이저 기술을 활용한 NFV 기술은 2005~2020년 현재까지도 현업에서 사용되고 발전하고 있는 기술이다. 그러나 NFV는 기업 단위 가상화 환경에서 시작된 기술이라 사용하면서 발생하는 성능 저하 및 클라우드 환경에서 운영하면서 단점이 발생했고, 이를 개선하기 위해 나온 기술이 CNF 기술이라고 할 수 있다. 클라우드가 본격적으로 사용되면서, 고객의 요구에 짧은 시간 안에 대응이 필요한 환경이 되고, 좀 더 경량화와 빠른 서비스가 가능하며, 동일 자원에 더욱 빠른 서비스를 제공하기 위해서 클라우드에 최적화된 영어로 Cloud Native 한 기술이 컨테이너 기술이라고 할 수 있다.

현재 클라우드 환경에서는 기존의 VM 기반 구조가 컨테이너 기반 구조로 빠르게 대체가 이루어지고 있는 상황이다. 여기에 대응하기 위해 네트워크 벤더에서도 컨테이너 기반의 네트워크 장비를 개발 중이거나 선별적으로 서비스에 적용해 테스트 중이라고 한다. 머지않은 장래에는 보다 용량이 줄어들고 부팅속도도 빠르며, 같은 조건의 VM에 비해 처리 성능이 늘어난 컨테이너 기반 방화벽이 클라우드 환경에서 많이 사용될 수 있을 거라 기대해 본다.

다음 호에서는 VPN(Virtual Private Network, 가상사설망)에 대해서 소개하도록 하겠다.