효율적인 하이브리드 클라우드 네트워크 모니터링 방안

네트워크 가시성 확보 통해 중복된 서비스·트래픽 헤어피닝 등 문제 해소해야


좌: 크리스탈 리(Crystal Li) 켄틱 제품 마케터
우: 짐 미한(Jim Meehan) 켄틱 제품 마케팅 이사
번역·감수: 조인호 시엔스 리드 기술 매니저
(kentik@sciens21.com)

클라우드 기술 중 네트워크 영역은 상당히 복잡하다. VPC, 클라우드 간 상호 연결, 여러 개의 가용 영역과 리전 등 새로운 개념들이 많다. 클라우드는 다른 클라우드 혹은 인터넷과 연결돼 하이브리드 및 멀티 클라우드 아키텍처를 형성하는데, 이때 빠른 구축 속도와 리소스 활용 방식에 대한 가시성 부족으로 인해 고비용 저효율이라는 실수를 저지르기 쉽다. 〈편집자〉

퍼블릭 클라우드의 네트워킹은 유사해 보여도 다르다. 기업들은 퍼블릭 클라우드 내 또는 퍼블릭 클라우드 간 네트워킹을 구축하기 위해 정교한 방법을 모색하고 있다.

그 이유는 ▲강력한 하이브리드·멀티 클라우드 아키텍처를 만드는 것 ▲멀티 클라우드 및 네트워크 공격에 대해 강력한 보안 기능을 구축하는 것 ▲더 높은 성능 및 가용성 요구 사항을 가진 클라우드 애플리케이션 지원 등 다양하다.

클라우드 네트워킹은 데이터센터로부터의 전환이 아니라 새로운 노하우다. 네트워킹 전문가이자 작가로 활동하는 이반 페펠냐크(Ivan Pepelnjak)는 "아마존웹서비스(AWS)의 세계에 처음으로 진입하는 전통적인 네트워크 엔지니어들은 종종 이상한 나라의 앨리스처럼 느낄 때가 있다"고 말한다. 이는 모든 것이 친숙해 보이면서도 한편으로는 모든 것이 이질적으로 보이기도 하는 것을 의미한다.

퍼블릭 클라우드 제공업체가 네트워킹 서비스를 기존 네트워크 하드웨어 공급업체와 다르게 설계한 것은 그럴 만한 이유가 있다. 이들은 기본적으로 대규모 환경에서도 원활히 작동하는 가상 네트워킹을 설계해야 한다. 퍼블릭 클라우드 제공업체는 기존 네트워크 공급업체와 달리 서비스에 실패할 경우 대중적인 평판 손상으로 이어질 수 있기 때문이다.

클라우드 전략은 클라우드 전문 지식을 필요로 한다. 퍼블릭 클라우드 내부 및 퍼블릭 클라우드 간 네트워킹을 구현하는 지식이 필요하며, 클라우드 네트워크는 초단시간 내 포화상태에 이를 수 있기에 퍼블릭 클라우드 제공업체는 네트워크 하드웨어 벤더들과 달리 모든 것을 바꿔야만 했다.

가시성 부족으로 비용 증가·서비스 중단 위험

최근 몇 년간 네트워크의 전략적 가치와 요구사항이 급격이 증가하는데 반해 네트워크를 모니터링하고 최적화하기 위한 도구들은 이러한 변화를 따라가지 못하고 있다. 이는 결과적으로 네트워크 성능 장애나 중단은 물론 비즈니스에 큰 영향을 미치는 결과로 이어질 수 있다. 또 원격 근무 증가에 따라 지금까지 감지할 수 없었던 네트워크 성능의 변화가 생산성에 영향을 미치는 것이 점점 가시화되고 있다.

대부분 5개 이상의 개별 네트워크 모니터링 도구가 있는 인프라 및 네트워크 팀들은 복잡한 인프라 전반의 네트워크 활동을 단일 뷰로 볼 수 없다. 이처럼 제한된 가시성으로 인해 민첩성이 저하되고 다음과 같은 문제점이 발생한다.

- 유사하나 관련 없는 데이터를 제시해 MTTR 악화
- 문제 예방에 사용되는 분석 인사이트 미흡
- 운영자가 계획 대신 네트워크 이슈 해결에 신경 써야 하므로 네트워크 중단 가능성 높아짐
- 네트워크 팀이 비즈니스 목표 변화에 대응해야 할 때 조직의 위험 증가

가시성은 모든 클라우드 네트워킹 전환 과정에서 필수적인 부분이며, 비용이 많이 발생되는 다섯 가지 실수를 방지할 수 있도록 지원한다.

■ 체크리스트 1: 중복된 서비스와 구별되지 않는 종속성

이러한 실수는 공유 아키텍처를 고려하지 않고 서로 단절된 여러 팀이 클라우드로 급격히 이동할 경우 발생한다. 서로 다른 팀이 클라우드에 별도의 애플리케이션을 구축한다고 가정해 보자.

각 팀은 컴퓨팅, 스토리지, 네트워크 구성 요소 등과 같은 클라우드 리소스를 가동시킨다. 그것들 중 다수는 실제로 재사용이 가능하고, 공유할 수 있다. 그중 일부는 DNS, 데이터베이스, 로드 밸런서 등과 같은 명백한 표준 서비스도 있다.

이는 단순히 클라우드 리소스를 복제하는 것만은 아니다. 정확히 동일한 기능을 수행하는 맞춤형 마이크로서비스가 중복되는 것을 볼 수 있다.

모든 팀이 협의 없이 빠르게 작업을 진행하므로 서로가 중복된 일을 하는지 알 수 없다. 곧 클라우드 환경은 얽히고설킨 상호 의존적인 웹서비스를 구성하게 될 것이다.

이처럼 가시성이 부족하면 취약한 아키텍처, 낭비되는 개발 노력, 막대한 클라우드 비용 지출 등과 같은 부정적인 결과가 발생할 수 있다.

또한 다음과 같은 시나리오도 발생할 가능성이 있다.

- A팀은 그들의 앱에 DNS 서비스를 설정한다. A팀의 DNS 서비스에 대해 알지 못하는 B팀도 그들의 앱에 대해 중복된 DNS 서비스를 만든다. 이 조직은 공유 인프라로 단일화할 수 있는 인스턴스에 대해 두 배의 비용을 지불하고 있다.
- 제3의 팀인 C팀도 그들의 앱을 위한 DNS 서비스가 필요하다. C팀은 서비스 환경을 알지 못한 채 B팀의 DNS를 사용하기 시작했다. 얼마 후, B팀은 A팀의 DNS 서비스에 대해 알게 됐고, 그것을 사용하면서 자신들의 서비스를 종료했다. C팀의 앱은 의존하던 서비스가 예고 없이 사라졌기 때문에 작동이 중단됐다.

클라우드 인프라의 유연성과 민첩성은 매우 뛰어나며, 개별 팀이 자체 앱을 빠르게 개발할 수 있게 할 수 있다는 장점이 있다. 그러나 중복을 발견하기 위한 가시성과 프로세스가 없다면 소프트웨어 개발 환경은 악화되고, 비용 및 신뢰성 문제가 발생할 가능성이 훨씬 더 높아지게 된다.

■ 체크리스트 2: 복잡한 트래픽 헤어피닝

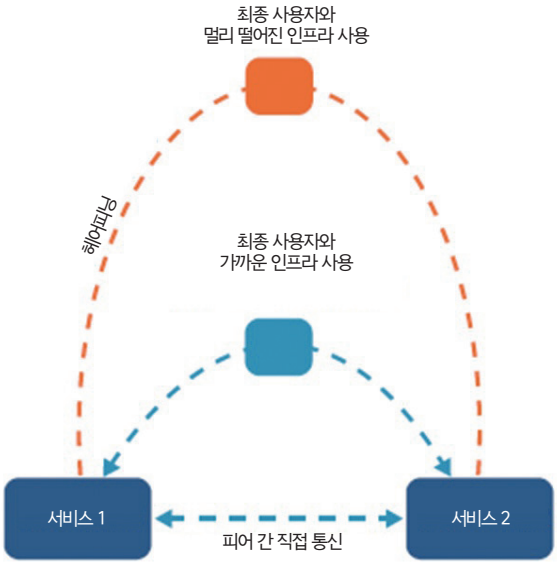
헤어피닝(hairpinning)이란 짧고 빠르며 저렴한 네트워크 경로를 통해 통신해야 하는 서비스가 지연 시간이 길고 비싼 경로를 통해 통신하게 될 때 발생하는 현상을 말한다. 그 원인과 특징은 다양하다. 두 가지 시나리오를 통해 알아보도록 한다.

첫 번째 시나리오에서는 물리적인 데이터센터 내 개별 영역에 두 개의 서비스를 배치한다고 가정한다. 잘못된 아키텍처 선택이나 단순한 IP 라우팅 구성 실수로 인해 이들 서비스 간의 통신 경로는 로컬 데이터센터 네트워크 패브릭 대신 클라우드 인터커넥트와 VPC를 경유한다.

이제 이러한 서비스가 통신할 때마다 훨씬 더 높은 대기 시간을 경험하고 있으며, 기가바이트(GB)당 값비싼 클라우드 데이터 전송 비용도 증가하고 있다. 반대로 클라우드에 배포된 두 개의 서비스 통신 경로 역시 로컬 데이터센터를 경유하는 경우도 포함된다.

두 번째 시나리오에서는 웹 프런트엔드, 애플리케이션 서버, 데이터베이스 백엔드로 구성된 서비스 체인을 상상해 보자. 데브옵스팀이 애플리케이션 서버를 클라우드로 마이그레이션했지만 웹 프런트엔드 및 데이터베이스는 여전히 레거시

〈그림 1〉 트래픽 헤어피닝



데이터센터에 존재한다. 이제 모든 웹 요청 시 클라우드 인터커넥션을 두 번 통과하는 일련의 호출이 발생하며, 이는 다시 성능 저하와 비용을 발생시키게 된다.

가시성이 부족하면 이와 같은 시나리오가 계속 반복될 수 있다.

■ 체크리스트 3: 불필요한 지역 간 트래픽

대부분의 클라우드 구성 요소가 사용한 만큼 지불하는 종량제 방식의 모델이라는 것은 비교적 잘 알려진 사실이다. 그러나 특정 구성 요소의 가격 세부 조건은 종종 이해되지 않는 경우가 있다. 예를 들면, 지역 간 데이터 전송의 GB당 비용이 지역 내 데이터 전송에 비해 훨씬 더 비싸다는 점이다.

〈그림 2〉처럼 지역 간 데이터 전송은 지역 내 데이터 전송 가격의 두 배에 달하는 것을 확인할 수 있다. 구글 클라우드 네트워크 가격 책정을 봐도 상황은 별반 다르지 않다. 그 차이는 최소 10배에 달한다.

- 동일 지역의 내 구역 간 송신 비용은 GB당 0.01달러
- 지역 간 송신의 경우에는 GB당 0.11~0.22 달러 범위로 다양하게 구성

클라우드 비용을 증가시키는 또 다른 실수도 존재한다. 바로 클라우드 설계자와 개발자들이 지역 간 불필요한 트래픽이 상당 수준 발생하도록 애플리케이션 또는 인프라를 구축한다는 사실이다. 관련 비용을 모른다면 누구나 이렇게 하기 쉽다. 클라우드 네트워크 비용을 간소화하려면 다음 세 단계를 수행하는 것이 권장된다.

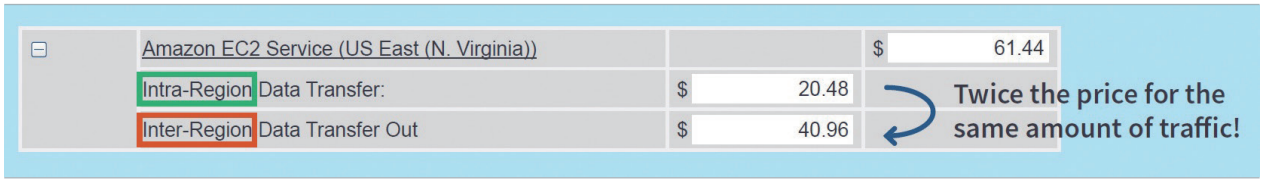
1. 식별: 지역 간 인터넷 송신 트래픽의 주요 기여자를 확인한다. 그리고 어떤 애플리케이션이 큰 대역폭 비용을 초래하고 있나? 어떤 애플리케이션 팀이 이 트래픽을 담당하고 있나? 불필요한 데이터 전송 요금에 포함돼 있나? 등과 같은 질문에 대한 답을 찾아야 한다.
2. 재배치: 인프라 내에서 이동 가능한 워크로드를 평가한다. 워크로드를 교체해 지역 간 통신을 최소화한다.
3. 통합: 모든 워크로드를 주의 깊게 검사하고 생성된 네트워크 트래픽을 이해한 다음 서로 결합 가능한 항목을 통합해 리소스를 절약해야 한다.

■ 체크리스트 4: 로컬 VPC에서 인터넷을 통한 클라우드 서비스 액세스

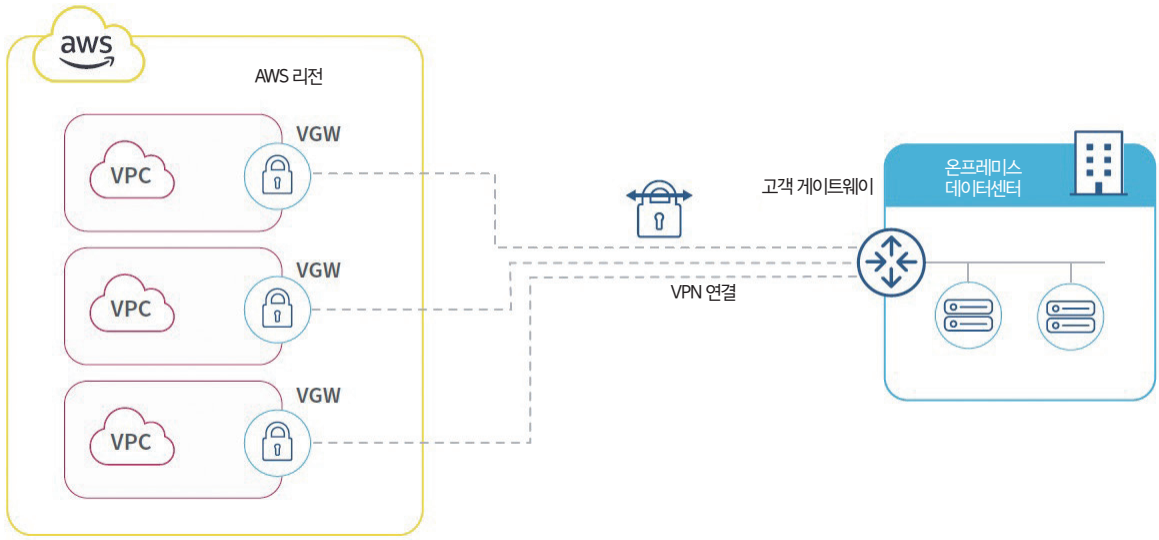
클라우드에서 애플리케이션을 구축하는 모든 사람은 기본 클라우드 서비스(예: 아마존 S3, 구글 클라우드 Pub/Sub, 애저 AD)를 처음부터 시작하는 것이 아니라 기본 클라우드 서비스를 빌딩 블록으로 사용함으로써 더 많은 노력을 기울일 수 있다는 것을 알고 있다.

이러한 서비스는 편리하고 시간도 절약되지만 시간당, 기가

〈그림 2〉 AWS 요금 계산기를 통해 산출한 계산



〈그림 3〉 로컬 VPC에서 인터넷을 통한 클라우드 서비스 액세스



비트 혹은 트랜잭션 당 가격표가 함께 제공된다. 또 규모에 따라 신속하게 누적될 수 있는 데이터 전송 비용이 있다는 점도 기억해야 한다. 좋은 소식은 현명한 운영자들이 이러한 비용을 상당히 줄이는 방법을 알고 있다는 것이다.

몇 가지 배경 지식은 이러한 비용을 더 잘 이해하는 데 도움이 된다. 우선 클라우드 공급자는 단일 지역에서 실행되는 서비스를 나타내는 IP 주소 범위를 사용해 인터넷에서 서비스에 액세스할 수 있도록 한다.

예를 들어, AWS us-west-1 지역에서 실행되는 S3 서비스는 3.5.160.0/22 주소 범위에서 인터넷에 공개된다. 이러한 서비스를 사용하기 위해 클라이언트는 서비스가 호스팅되는 IP 범위로 [sms.eu-west3.amazonaws.com](http://sms.eu-west-3.amazonaws.com/)과 같은 DNS 이름을 확인하게 된다. 그런 다음 쿼리에서 반환된 IP 주소로 트래픽을 전송한다.

클라우드 엔지니어가 새로운 VPC를 설정할 때 트래픽이 로컬이 아닌 대상으로 전달되는 방식을 결정하는 라우팅 규칙도 설정해야 한다. 인터넷에 바인딩 된 트래픽은 항상 게이트웨이 장비를 가리키는 기본 경로를 따른다. 이러한 장치를 통과하는 트래픽은 인터넷 송신 트래픽으로 정의되고, 여기에는 VPC 인스턴스와 동일한 지역 또는 영역에 있는 트래픽도 포함해 클라우드 서비스에만 연결하기 위해 인터넷으로 이동하는 트래픽이 포함된다. 이러한 비용은 시간이 지남에 따라 누적되며 큰 폭으로 증가하게 된다.

다행히도 대부분의 클라우드 공급업체들이 일반적으로 '엔드포인트 서비스'라 불리는 기능을 출시했다. 이러한 트래픽은 공용 인터넷으로부터 멀리 떨어져 있으므로 인터넷을 통한 트래픽 전송과 관련된 데이터 전송 비용과 보안 위험을 모두 줄일 수 있다. 엔드포인트 서비스를 사용하면 사용자는 VPC 서브넷 내부의 사설 IP 주소를 이용해 로컬 네트워크 인터페이스를 구성할 수 있다.

이러한 인터페이스는 구성된 엔드포인트 서비스를 향하는 모든 트래픽에 대해 프록시 역할을 한다. 그 결과 서비스에 대한 트래픽은 낮은 송신 가격으로 로컬 및 비공개로 유지된다.

예를 들어, us-east-1의 VPC에서 us-east-1에서 호스팅되는 AWS 서비스로의 트래픽은 $0.02/GB다. 대부분의 회사 규모로는 큰 문제가 아니다. 그러나 매월 50TB를 S3로 전송할 경우 이러한 비용은 월 1000달러를 빠르게 초과할 수 있다. 이 트래픽을 S3로 연결하도록 VPC 엔드포인트를 설정하면 비용을 상당히 절감할 수 있다.

VPC 엔드포인트 요금에는 시간당 $0.01이 포함되며, 인터페이스당 $0.01이 넘는 모든 데이터는 GB당 $0.01이 청구된

다. 즉 AWS 프라이빗링크(PrivateLink) 엔드포인트를 통해 S3로 전송된 동일한 50TB의 비용이 월 약 520달러(표준 인터넷 전송 요금보다 50% 절감)가 소요된다.

■ 체크포인트 5: 기본 인터넷 트래픽 전송 사용

클라우드 공급자의 기본 인터넷 사용법은 분명 쉽지만, 기업이 수많은 비트(Bit)를 제공해야 할 때 비용이 빠르게 증가할 수 있다. 비용은 GB당 기존 IP 전송보다 10배 이상 비쌀 수 있다. 다른 트래픽 전송 옵션을 고려하고 구현하지 않으면 클라우드 마이그레이션으로 인해 엄청난 과금이 발생할 수 있다.

이를 줄이기 위한 첫 번째 단계는 어떤 앱이 인터넷에 트래픽을 얼마나 제공하는지 목록을 작성하는 것이다. 팀은 비용 영향을 알지 못하기 때문에 기본 인터넷 송신 기능을 사용해 새 앱을 배포할 수 있다. 그렇기 때문에 트래픽에 대해 목록을 작성하는 것은 비용을 제어하는 대단히 중요한 방법이다.

다음은 인터넷 송신요금을 줄일 수 있는 몇 가지 트래픽 전송 옵션들이다.

- **CDN(Contents Delivery Network) 활용**: 전 세계에 분산된 노드에서 자주 요청되는 객체를 캐시 할 수 있으므로, 최종 사용자가 원본 서버에서 직접 사용자에게 서비스를 제공하는 것보다 GB당 훨씬 저렴한 비용으로 트래픽을 제공할 수 있으며, 성능(지연 시간)도 훨씬 우수하다. 클라우드 공급업체는 타사 공급업체와 함께 자체 CDN 서비스를 제공한다.
- **모바일용 앱 내 패키지**: 모바일 앱과 상호 작용하는 클라우드 서비스의 경우 네트워크를 통해 서비스를 제공하는 대신 앱의 일부로 상대적으로 정적인 큰 개체를 패키징 하는 것을 고려해야 한다.
- **비공개 발신**: 많은 트래픽을 생성하는 서비스의 경우, 클라우드 상호 연결을 통해 상대적으로 저렴한 IP 전송에 잘 연결된 PoP로 백홀(backhaul)하는 것이 더 경제적일 수 있다. 이는 이미 PoP가 있는 네트워크와 기존의 물리적 데이터센터를 위한 중계망에 매력적이다.

하이브리드 클라우드 가시성 격차 해소

조직이 하이브리드, 멀티 클라우드 환경을 채택함에 따라 네트워크 및 인프라 팀은 문제를 식별하고 해결하는 능력에 영향을 미치는 분리된 도구로 심각한 사각지대에 직면하게 된다.

켄틱(Kentik)은 하이브리드 클라우드 환경에서 도입된 운영 격차를 해소하는 솔루션으로, 프라이빗 클라우드와 퍼블릭 클라우드를 모두 포함해 인프라 전반에 걸쳐 시각화를 제공한다. 네트워크 팀은 클라우드 및 데이터센터 환경의 VPC 플로우, 서브넷, 이스트-웨스트(East-West) 트래픽 문제를 해결하고, 장비 인터페이스 상태를 확인할 수 있다.

인터넷 및 WAN 엣지 영역에서 켄틱은 VPN 및 방화벽 보안 영역을 통한 플로우 모니터링, 용량 계획, 성능 최적화 및 감사(Audit) 기능을 제공한다.

켄틱의 주요 특징은 다음과 같다.

- **하이브리드 클라우드 양 측면에 대한 가시성 확보**: 인터넷을 포함한 여러 클라우드에서 네트워킹을 실시간으로 매핑할 수 있으며, 클라우드 제공업체, 지역, 가용 영역, VPC, 서브넷 및 인스턴스로의 트래픽에 대한 모든 세부 정보를 시각화한다.
- **클라우드 네트워킹 비용 최적화**: 클라우드 트래픽 비용을 최적화하고 제어한다. 비용을 흐름별로 세분화해 분석하고 계정, VPC, 서브넷, 인스턴스 또는 기타 트래픽 특성별로 고가의 트래픽 흐름을 분석한다. 또 유용한 보고서를 생성하고, 비용 메트릭을 대시보드에 통합하며, 고가의 트래픽에 대한 알림을 받을 수 있다.
- **사전 예방적 모니터링 및 신속한 문제 해결**: 클라우드 문제를 모니터링하고 문제를 해결할 수 있도록 돕는다. 데이터센터 및 퍼블릭 클라우드 환경의 성능을 확인하고 자세히 알아볼 수 있으며, 지속적인 통합 테스트에서 클라우드 성능 문제에 대한 경고를 제공한다. 뿐만 아니라 보안 및 규정 준수 정책, 네트워크 용량, 연결 유형 및 지리적 위치 고려사항까지 확인 가능하다.