DNS 는 왜 다시 경영 의제가 되었는가: 정적 인프라의 한계와 F5 의 해법

DNS 가 멈추면 애플리케이션도 멈춘다

애플리케이션 가용성을 논할 때 대부분의 조직은 서버, 네트워크, 스토리지의 이중화부터 점검합니다. 하지만 그 앞단에는 반드시 거쳐야 하는 관문이 있습니다. 바로 DNS입니다. 사용자의 모든 요청은 DNS 해석을 통과해야만 목적지에 도달할 수 있고, 이 관문이 응답하지 않으면 뒤에 있는 인프라가 아무리 견고해도 서비스는 열리지 않습니다.

F5는 백서 「The Dynamic DNS Infrastructure」에서 이 구조를 다음과 같이 정리합니다.

> *"인터넷이 작동하지 않으면 DNS도 작동하지 않고,*
> *DNS가 작동하지 않으면 애플리케이션도 작동하지 않는다."*

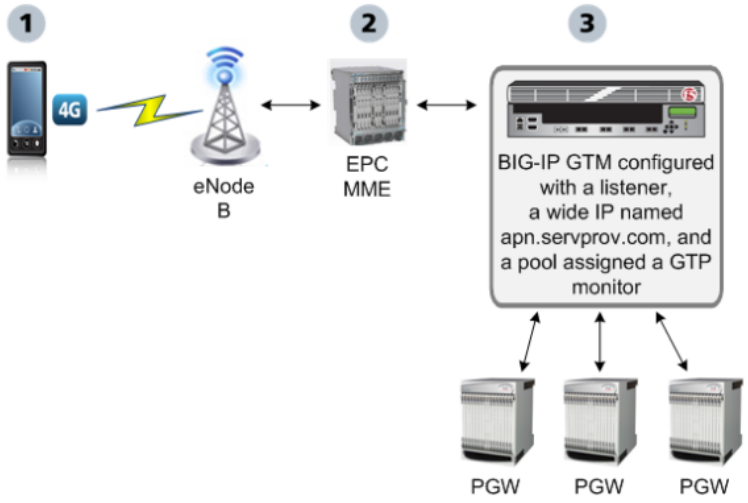
단순한 문장이지만, 포함된 의미는 무겁습니다. DNS는 기업이 보유한 인프라 가운데 가장 공개적이고, 가장 광범위하게 의존되며, 동시에 가장 방치되기 쉬운 계층이라는 것입니다.

트래픽은 왜 계속 늘어나기만 할까?

DNS 인프라에 가해지는 첫 번째 압박은 규모입니다. ITU(국제전기통신연합)의 「Facts and Figures 2025」 1)에 따르면 **2025년 기준 전 세계 인구의 74%, 약 60억 명이 인터넷을 사용 중**이며, 이 비율은 2024년 71%에서 1년 만에 3.3%p 상승했습니다. DNS 트래픽도 같은 방향으로 움직입니다. APNIC의 분석2)에 따르면 NS1의 관리형 DNS 고객 트래픽만 집계해도 **3개월간 7.5조 건의 DNS 쿼리가 발생했고, 초당 평균 처리량은 100만 건**에 달했습니다. 웹페이지 자체도 계속 복잡해지고 있습니다. HTTP Archive의 「Web Almanac 2025」 3)에 따르면 데스크톱 페이지의 55%가 2개 이상, 39%가 3개 이상의 서드파티 트래커와 연결되는데, 트래커 하나하나가 별도 도메인에 대한 DNS 조회를 요구합니다.

방향은 지금도 동일합니다. 모바일 트래픽, IoT 디바이스, 마이크로서비스 아키텍처는 DNS 조회 빈도를 지속적으로 밀어올리는 요인이며, 쿼리량이 늘어날수록 여유 용량과 응답 속도는 서비스 전체의 병목이 될 가능성이 커집니다. DNS는 눈에 띄지 않지만, 방치한 결과는 결코 조용히 지나가지 않습니다.

보안은 왜 별개의 문제가 아닐까?



출저: F5

트래픽 증가와 별개로, **DNS는 공격 표면으로서도 취약합니다**. 백서는 DNS를 DDoS 공격의 두 번째 주요 벡터로 지목하며, 피싱과 중간자(MITM, Man-in-the-Middle) 공격의 출발점으로도 지적합니다. 개별 애플리케이션의 장애는 해당 서비스에만 영향을 미치지만, DNS 장애는 데이터센터 전체의 서비스를 동시에 무력화시킨다는 점에서 파급 범위 자체가 다릅니다.

기존 대응책이었던 DNSSEC(DNS Security Extensions)도 완전한 해법은 아니었습니다. 정적 DNSSEC 구현은 **월 1회 수준의 서명 주기**와 **지리적 위치 정보**, 서명·검증 과정에서 발생하는 **연산 오버헤드**라는 세 가지 한계를 안고 있었습니다. Infoblox 아키텍처 부사장 Cricket Liu는 백서에서 이렇게 진단합니다.

"고성능 DNSSEC 검증 솔루션은 더 많은 사이트가
DNSSEC을 배포하면서 매우 중요해질 것이다.

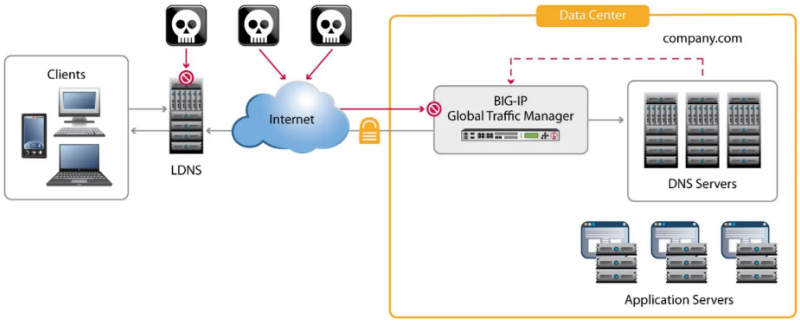
라운드로빈만으로 충분한 시대는 끝났다

전통적인 DNS 부하분산 방식인 **라운드로빈**(Round Robin)**은** 요청을 순차적으로 분배할 뿐, **대상 서버의 상태나 사용자의 지리적 위치를 전혀 고려하지 않습니다**. 장애가 발생한 서버로도 트래픽이 전달될 수 있다는 뜻입니다. 트래픽 증가와 보안 위협이라는 두 압박이 동시에 커지는 지금, 이 방식은 구조적 한계에 부딪힙니다. 정적인 규칙으로는 동적인 위협을 막을 수 없습니다.

F5 의 해법: 정적 DNS 에서 동적 DNS 로

F5는 2002년부터 DNS 및 글로벌 애플리케이션 전달 솔루션을 제공해 왔으며, BIG-IP DNS(구 GTM, Global Traffic Manager)는 이 문제를 전체 프록시(Full Proxy) 아키텍처로 풀어냅니다. 핵심은 응답을 고정하지 않는다는 것입니다. 실시간 상태에 따라 매 순간 동적으로 결정합니다.

가용성 측면에서는 **5초 주기의 상태 모니터링으로 장애 서버를 자동으로 제외**하고, 글로벌 서버 로드밸런싱(GSLB, Global Server Load Balancing)으로 사용자를 지리적으로 가장 가까운 정상 데이터센터에 연결합니다. 여러 BIG-IP DNS 시스템이 Sync Group으로 상태 정보를 실시간 공유하기 때문에, 어느 시스템에 쿼리하더라도 동일하게 최적화된 응답을 받을 수 있습니다.



출처: F5

보안 측면에서는 **DNSSEC 서명을 실시간·동적으로 수행해** 지리위치 기반 라우팅과 보안을 동시에 구현하고, **IP Anycast와 전체 프록시 아키텍처로 DDoS 트래픽을 분산**시키며 비정상 요청을 걸러냅니다. 서명키는 FIPS 140-2 Level 3 인증 하드웨어 모듈에 저장할 수 있어, 미국방부 수준의 DNSSEC 의무화 요건에도 대응 가능합니다.

성능 측면에서는 **DNS Express가 인메모리 엔진으로** 권한 있는 DNS 응답을 처리해 기존 DNS 서버 대비 응답 속도를 끌어올리고, **캐싱 효율화를 통해 아웃바운드 DNS 쿼리를 최대 80%까지 줄일 수 있습니다**. DNSSEC 검증에 필요한 암호화 연산도 클라이언트가 아닌 BIG-IP가 대신 처리해 부담을 낮춥니다. 다만 이는 DNSSEC 자체의 연산 오버헤드가 업계 전반에서 해소됐다는 뜻은 아니며, BIG-IP를 통해 해당 조직만 그 부담에서 벗어난다는 의미입니다.

확장성 측면에서는 **멀티코어 아키텍처를 기반으로** 대규모 엔터프라이즈 **트래픽에 선형적으로 대응하며**, 물리·가상 데이터센터가 혼재된 환경이나 VMware vSphere, Microsoft Hyper-V, Citrix XenServer 등 가상화 플랫폼, 나아가 **IPv4-IPv6 전환기의 DNS64/NAT64 요구까지** 하나의 플랫폼에서 수용합니다.

의사결정권자는 무엇을 판단해야 할까?

DNS 인프라 투자는 흔히 후순위로 밀립니다. 눈에 보이는 장애가 드물기 때문입니다. 하지만 지금까지의 논의가 보여주는 구조는 분명합니다. 트래픽과 공격 표면은 구조적으로 계속 증가하고, DNS 장애의 파급 범위는 개별 서비스가 아닌 데이터센터 전체이며, 기존의 정적 방식(라운드로빈, 정적 DNSSEC)은 이 증가분을 감당하도록 설계되지 않았습니다.

반대로 동적 DNS 인프라는 가용성, 보안, 성능, 확장성이라는 네 축에서 동시에 리스크를 낮추고, 쿼리 80% 절감이라는 비용 효율까지 확보할 수 있는 영역입니다. ROI를 계량화하기 상대적으로 명확한 투자 항목이라는 뜻입니다.

질문은 "투자할 것인가"가 아니라 "언제 투자할 것인가"입니다.

본 솔루션 도입·평가와 관련된 질문은 grometric@grometric.kr 로 문의해 주세요.

참고자료

1) https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-use/

2) https://circleid.com/posts/20230316-analysis-of-7.5-trillion-dns-queries-reveals-public-resolvers-dominate-the-internet

3) https://almanac.httparchive.org/en/2025/privacy