백서

DDoS 공격에 대해 안정성과 가용성을 유지할 수 있는 DNS 구축하기

서론

Edge DNS는 기업의 웹사이트 및 기타 애플리케이션과 사용자를 연결할 수 있도록 권한 DNS 서비스를 제공합니다. 많은 기업들이 성능에는 큰 관심을 기울이지만 DNS의 안정성 및 가용성은 간과하는 경우가 빈번합니다. 하지만 DDoS 공격으로 인해 서비스가 중단되고 사용자 접속이 차단되는 것을 막기 위해 DNS는 매우 중요합니다. Akamai의 Edge DNS는 독보적인 글로벌 확장성, 분리된 IP Anycast 아키텍처, 다양한 DDoS 제어 기능, 다른 Akamai 서비스를 활용할 수 있는 기능을 갖추고 있으며 대규모 DDoS 공격에도 가용성을 유지할 수 있도록 설계되었습니다. Edge DNS는 매니지드 DNS 서비스로, 기업과 사용자를 항상 연결하기 위해 최적의 성능과 가용성을 제공합니다.

통계

Akamai는 원래 글로벌 CDN(콘텐츠 전송 네트워크) 솔루션을 지원하는 권한 DNS 서비스를 제공하기 위해 Edge DNS를 구축했습니다. 지난 몇 년 동안 대규모 DNS 인프라의 확장성을 높이고 가용성을 유지하는 가장 효과적인 방법에 대해 많은 교훈을 얻었습니다. 오른쪽 통계를 보면 Akamai 플랫폼의 규모를 확인할 수 있습니다. 하지만 통계만으로는 가용성과 안정성에 대한 의미 있는 정보를 확인할 수 없습니다. 플랫폼 아키텍처, 특정 DDoS 방어 능력, 공격으로부터 플랫폼을 보호하기 위해 Akamai가 사용할 수 있는 전체 용량을 함께 고려해야 합니다.

플랫폼 통계

- 수천 개의 네임 서버
- 1,000여 개의 PoP
- 140여 개 도시
- 40여 개 국가

Akamai는 보안상의 이유로 네임 서버 수, 숫자, 위치, PoP(points of presence) 규모에 대한 구체적인 세부 정보를 공개하지 않는 정책을 갖고 있습니다. 이런 정보를 이용한 공격 시도로부터 Akamai와 고객들을 보호하기 위해서입니다.

아키텍처

위 통계에서 볼 수 있듯이, Edge DNS는 현재 시장에서 가장 경쟁력 있는 권한 DNS 서비스보다 확장성이 뛰어납니다. 하지만 서버 수, PoP, 총 네트워크 용량에 대한 개괄적인 통계 자료는 글로벌 플랫폼의 가용성 및 안정성 수준을 파악하기에 충분하지 않습니다. Akamai가 특별히 설계한 Edge DNS는 기존에 성능에만 초점을 맞춘 다른 DNS 솔루션과 차별화되는 성능을 갖췄을 뿐만 아니라 DDoS 공격에 대비하여 가용성 및 안정성을 제공하며, 네임 서버, PoP, 네트워크, 분리된 IP Anycast 클라우드를 비롯하여 여러 단계에서의 이중화를 지원합니다.

IP Anycast

Edge DNS는 IP Anycast 모델을 사용하는 1,000개 이상의 PoP에 배포된 수천 개의 네임 서버로 구성되어 있고 DNS 쿼리에 응답합니다. IP Anycast는 사용자의 쿼리를 가장 가까운 PoP로 전달해 리졸브합니다. 성능이 더 우수할 뿐만 아니라 근본적으로 가용성 및 안정성을 강화할 수 있기 때문에 대부분의 권한 DNS 서비스가 IP Anycast를 사용합니다.

- **가용성** - IP Anycast를 사용하면 서로 다른 네트워크 위치에 있는 네임 서버가 하나의 IP 주소에 대한 쿼리에 응답할 수 있습니다. Edge DNS는 IP Anycast를 활용하여 여러 데이터센터에서 DNS 레졸루션을 제공할 뿐만 아니라 전 세계적으로 부하를 분산해 가용성을 개선합니다. 또한 개별 물리적 서버 또는 전체 PoP는 도메인 레졸루션의 전반적인 기능에 영향을 주지 않고 오프라인 상태가 될 수 있습니다.
- **확장성** - Edge DNS 인프라는 수많은 PoP 에 걸쳐 배치된 수많은 물리적 서버로 구성됩니다. 많은 기업들이 대규모 DNS 요청에 응답할 때 필요한 방대한 컴퓨팅 리소스를 제공합니다. 또한 Edge DNS는 기타 Akamai 서비스와 용량을 공유하기 때문에 많은 PoP에서 상당한 규모의 추가 네트워크 용량에 접속할 수 있습니다. 따라서 Edge DNS는 독립형 DNS 서비스보다 확장성이 훨씬 우수하고 DNS Flood 및 다른 종류의 DDoS 공격에 대응할 수 있습니다.
- **분산** - IP Anycast를 사용하면 확장성이 더 우수할 뿐만 아니라 Edge DNS가 여러 PoP와 다양한 네트워크 위치 전반에 걸쳐 트래픽을 분산할 수 있습니다. 이러한 PoP에 대한 지리적 위치와 네트워크 배포를 신중하게 고려하면 특정 지역 또는 네트워크에 대한 소규모 공격의 영향을 줄이고 다른 지역의 클라이언트 시스템에 대한 가용성을 유지하는 데 도움이 됩니다.

Akamai만 IP Anycast를 사용하는 것은 아닙니다. IP Anycast는 여러 네임 서버가 사용자의 DNS 쿼리를 확인하도록 하여 모든 DNS 서비스에 대한 네임 레졸루션 가용성을 개선합니다. 하지만 IP Anycast를 사용하더라도 플랫폼의 전체 규모로 인해 안정성이 제한적이고 대규모 DDoS 공격은 여전히 클라우드 기반 플랫폼에 과부하를 발생시킬 수 있습니다. 게다가 아키텍처가 다양하지 않은 상태에서는 소규모 공격이 특정 지역의 DNS 서비스를 다운시켜 많은 사용자들이 서비스를 사용할 수 없게 만들고 해당 사용자가 접속하는 모든 웹사이트의 가용성에 영향을 미칠 수 있습니다.

Edge DNS 클라우드

Edge DNS는 공격에 대한 안정성을 더욱 개선하기 위해 네임 서버와 PoP를 여러 IP Anycast 클라우드로 분할합니다. Edge DNS 클라우드는 전용 네임 서버, PoP, 관련 네트워크 용량 및 연결로 구성됩니다. 모든 클라우드는 서로 독립적으로 운영되며, Edge DNS는 가용성, 확장성, 분산 측면에서 여러 독립형 DNS 제공업체와 동일합니다.

Edge DNS IP Anycast 클라우드는 다양한 아키텍처 집합입니다. 동일한 클라우드는 존재하지 않지만, 모든 클라우드는 두 가지 설계 원칙, 즉 성능과 가용성 측면에서 전반적으로 일치합니다.

- **성능** - 성능 클라우드는 전 세계에 분포된 100개가 넘는 PoP를 보유할 수 있고 각각의 PoP는 일련의 네임 서버로 구성되어 있습니다. 그림 1에서 볼 수 있듯이, 성능 클라우드는 더 빠른 룩업(lookup) 시간과 더 나은 성능을 제공하기 위해 사용자 및 로컬 인터넷 서비스 사업자(ISP)와 가까운 여러 위치에 소규모 네임 서버 클러스터를 구축합니다. PoP의 규모가 작으면 DDoS 공격에 취약할 수 밖에 없고 컴퓨팅 리소스와 네트워크 용량이 감소합니다.
- **가용성** - Edge DNS는 많은 가용성 클라우드를 유지합니다. 그림 1에서 볼 수 있듯이, 가용성 클라우드는 보유한 PoP의 수는 적지만, 중앙화된 데이터센터에 수백 개의 네임 서버를 구성할 수 있으며 상당한 전용 네트워크 용량과 여러 네트워크 연결을 지원하는 하나 이상의 앵커 지역을 포함합니다. 앵커 지역은 DNS 요청 및 기타 네트워크 트래픽의 급격한 증가에 대응할 수 있는 확장성을 갖춘 가용성 클라우드를 제공합니다. 가용성 클라우드는 규모와 숫자가 더 작은 PoP로 앵커 지역을 강화하여 전 세계 사용자에게 적합한 수준의 성능을 유지합니다.

그림 1: Edge DNS는 여러 DNS 클라우드를 다양한 아키텍처와 결합하여 DDoS 공격에 대한 성능, 안정성, 가용성을 최적의 조합으로 제공합니다.

세그먼트된 아키텍처

Edge DNS는 단일 IP Anycast 클라우드에서 권한 DNS 서비스를 운영하는 다른 사업자와 비교할 때 근본적으로 다른 수준의 가용성을 제공합니다. 전체 플랫폼이 아닌 특정 지역에만 영향을 미칠 수 있는 소규모 공격이 발생했을 때 IP Anycast는 서비스의 전반적인 업타임을 유지함으로써 모든 사업자들에게 가용성 혜택을 제공합니다. 하지만, 특정 지역에서 발생한 서비스 장애라 하더라도 피해를 입은 지역의 최종 사용자뿐만 아니라 이러한 사용자들과 연결하기 위해 해당 서비스에 의존하는 기업에게도 영향을 미칩니다. 게다가, 대형 DDoS 공격이 전 세계의 공격 시스템에서 생성된 트래픽과 동시에 발생하면 전체 플랫폼에 장애가 발생할 가능성이 있습니다.

Edge DNS는 많은 수의 다양한 IP Anycast 클라우드를 보유하고 있기 때문에 1개 이상의 클라우드가 다운되더라도 지속적으로 작동합니다. 이는 단일 클라우드 아키텍처에 비해 DDoS 공격에 대한 높은 수준의 가용성과 안정성을 제공합니다. 또한 여러 개의 IP Anycast 클라우드를 운영하는 경우에는 전체 플랫폼의 하위 섹션 전반에 걸쳐 트래픽을 분할하므로 광범위한 DDoS 공격으로 인한 영향을 줄일 수

있다는 장점이 있습니다. 예를 들어, 단일 Edge DNS IP Anycast 클라우드에 대한 공격은 해당 특정 클라우드를 구성하는 물리적 네임 서버 및 PoP로 이동됩니다. 분할된 아키텍처는 다른 IP Anycast 클라우드에서 발생한 영향을 격리하여 개별 클라우드 또는 고객이 DDoS 공격을 받고 있더라도 Edge DNS가 모든 지역에서 플랫폼 가용성을 유지할 수 있도록 합니다.

그림 2: 모든 Edge DNS 고객은 성능 및 가용성 클라우드의 고유한 조합을 기반으로 네임 서버를 수신하여 다른 고객에게 발생한 공격으로 인한 부수적인 피해를 최소화합니다.

Edge DNS의 세그먼트된 아키텍처는 전반적인 플랫폼 안정성을 향상시킬 뿐만 아니라 다른 고객이 사용하는 네임 서버가 공격을 받는 경우 부수적인 피해 리스크를 줄입니다. Edge DNS는 모든 고객에게 여러 Edge DNS 클라우드를 할당하며, 해당 클라우드는 다른 어떤 고객과도 공유되지 않는 성능과 가용성 클라우드의 고유한 조합으로 구성됩니다. 그림 2에서 볼 수 있듯이, 이 배포 방식은 두 고객 사이에 네임 서버와 IP Anycast 클라우드가 겹칠 가능성을 최소화합니다. 또한, 다른 고객에게 할당된 IP Anycast 클라우드가 대규모 DDoS 공격의 표적이 되는 경우에도 사용 가능한 네임 서버를 모든 고객에게 제공합니다.

고객 위임 관리

단일 기업을 대상으로 여러 건의 DDoS 공격이 긴 기간에 걸쳐 발생하기도 합니다. Akamai는 광범위하고 지속적인 공격 캠페인이 몇 개월 동안 계속되는 것을 관측해 왔습니다. 이러한 상황에서 Akamai가 설계한 Edge DNS의 세분화된 아키텍처는 공격의 표적이 아닌 고객에게 미치는 영향을 최소화할 수 있는 뛰어난 유연성을 제공합니다. 그림 3에서 볼 수 있듯이, Akamai는 개별 고객의 클라우드를 재할당하고 필요한 경우 공격의 영향을 추가로 격리할 수 있습니다.

그림 3: Akamai는 네임 서버 위임을 관리하여 공격의 표적이 된 고객을 개별 클라우드 밖으로 이동시키고 공격의 표적이 아닌 고객에 대한 중복을 최소화하는 등 공격의 영향을 더욱 최소화할 수 있습니다(위의 그림 2 참조).

세부 내용은 다음과 같습니다.

- **표적이 된 고객을 특정 클라우드 밖으로 이동** - 모든 Edge DNS 고객은 다른 고객과 IP Anycast 클라우드를 공유합니다. 따라서 한 고객의 Edge DNS 클라우드를 표적으로 하는 공격은 다른 고객에게 할당된 클라우드의 가용성에 영향을 미칠 수 있습니다. 정상적인 상황에서는 리커시브 리졸버가 자동으로 고성능 클라우드로 전환됩니다. 하지만 공격 캠페인이 계속되면 Akamai는 해당 공격을 받고 있는 고객의 IP Anycast 클라우드를 재할당하여 공격을 받지 않는 고객의 가용성을 복원할 수 있습니다.
- **표적이 아닌 고객을 위해 중복 최소화** - 여러 Edge DNS 고객이 정상적인 것보다 더 많은 수의 Edge DNS 클라우드를 공유할 수 있습니다. 이 경우 전체 서비스의 가용성은 유지되지만 단일 고객에 대한 대규모 공격이 다른 고객의 클라우드 성능에 상당한 영향을 미칠 수 있습니다. 필요한 경우 Akamai는 공격의 표적이 아닌 고객을 위해 클라우드를 재할당하여 공격의 표적이 된 고객과의 중복을 줄이거나 없애고 최종 사용자를 위해 성능을 복원할 수 있습니다.

다양한 서버 배치

Akamai는 각 Anycast 클라우드 내에서 클라우드의 전반적인 안정성을 높이기 위해 다양한 위치에 물리적 네임 서버를 구축합니다. 다양한 Edge DNS 클라우드 위치는 세그먼트된 또 다른 트래픽 계층을 서로 다른 네트워크에 제공하여 다양한 상황에서 가용성을 극대화합니다. 구체적인 사례는 다음과 같습니다.

- **여러 네트워크가 있는 데이터센터** - DDoS 공격을 방어하는 안정성을 고려할 때 네트워크 연결의 다양성은 용량만큼 중요할 수 있습니다. 대규모 DDoS 공격은 데이터센터에 도달하기 전에 업스트림 ISP 및 기타 네트워크에 과부하를 발생시키므로 데이터 센터 자체에 영향을 미치지 않더라도 네트워크가 혼잡해지고 서비스에 장애가 발생할 수 있습니다. Edge DNS는 공격이 진행되는 동안 최종 사용자의 DNS 쿼리에 응답하는 기능과 가용성을 유지하기 위해 대규모 데이터센터에 네임 서버를 구축하고 여러 네트워크를 통해 상당한 용량과 연결을 제공합니다.
- **ISP 격리** - 대부분의 경우 Edge DNS는 개별 ISP의 네트워크에 직접 네임 서버 클러스터를 구축합니다. 이러한 네임 서버는 해당 네트워크 내에서만 IP Anycast 트래픽을 브로드캐스트하고 해당 ISP의 최종 사용자에 대해서만 DNS 쿼리를 리졸브합니다. 이러한 방식은 네임 서버의 특정 클러스터가 서비스할 수 있는 최종 사용자 수를 제한하지만, IP Anycast 클라우드가 해당 ISP 외부로부터 공격을 받을 때 해당 사용자의 가용성을 유지합니다. 공격자가 이러한 네임 서버를 보려면 특정 ISP 네트워크에 시스템을 보유해야 하며, 심지어 가용 용량만으로 클라우드 하나를 충분히 보호할 수 있는 경우도 있습니다.
- **네트워크 다양성** - 고객에게 의도적으로 여러 클라우드를 할당합니다. 특정 ISP에 서버를 갖고 있는 클라우드도 있고 보다 광범위한 연결 시스템을 갖고 있는 클라우드도 있습니다. 이 아키텍처는 지정된 클라이언트의 리커시브 네임 서버가 사용 가능한 Edge DNS 클라우드에 항상 연결할 수 있도록 보장합니다.

- **기타 Akamai 서비스와 공유되는 데이터센터** - 권한 DNS를 넘어 많은 다양한 서비스를 운영함으로써 Akamai는 여러 서비스를 지원하는 데이터센터에 Edge DNS 네임 서버를 구축할 수 있습니다. 아래에서 자세히 설명된 바와 같이, 이를 통해 Edge DNS는 대규모 DDoS 공격에 대응할 때 방대한 네트워크 용량에 접속할 수 있고 전용 네트워크 용량 및 Akamai가 이미 다른 서비스를 위해 갖고 있는 퍼블릭 피어링 환경에도 접속이 가능합니다.

DDoS 제어

Edge DNS는 아키텍처 설계 외에도 DNS Flood라는 DDoS 공격의 영향을 줄이는 데 도움이 되는 여러 제어 기능을 제공합니다. 많은 DDoS 공격이 네트워크 링크에 과부하를 발생시키기 위해 대량 트래픽을 사용하는 반면, DNS Flood는 정상적인 DNS 요청을 대량으로 생성하여 물리적 네임 서버에서 컴퓨팅 및 메모리 리소스를 소비하고 실제 최종 사용자의 쿼리에 응답할 수 없도록 만듭니다. Akamai는 여러 가지 방법으로 DNS Flood로부터 Edge DNS 플랫폼을 보호합니다.

- **확장성** - Akamai의 권한 DNS 서비스의 규모는 경쟁사의 다른 DNS 솔루션 대비 몇 배 더 큽니다. Edge DNS는 전 세계적으로 1,000개가 넘는 PoP에 구축된 수천 개의 네임 서버를 활용합니다. 명확한 의미의 DDoS 제어는 아니지만, IP Anycast는 공격 트래픽을 지역과 네트워크 전체에 분산시키고, 물리적 네임 서버 수는 크게 급증한 DNS 요청 수를 흡수하는데 필요한 컴퓨팅 및 메모리 리소스를 Edge DNS에 충분히 제공합니다.

- **전송률 제한** - Edge DNS는 전송률 제한 기능을 포함하고 있으며 요청 건수가 설정된 임계값을 초과할 경우 개별 IP 주소의 요청을 자동으로 삭제할 수 있습니다. 전송률 제한은 DNS 요청이 크게 급증하여 물리적 네임 서버에서 컴퓨팅 및 메모리 리소스를 소비하는 것을 방지하며, 요청을 대량으로 생성하지만 상대적으로 낮은 대역폭을 사용하는 공격에 대응할 때 유용합니다. Edge DNS의 전송률 제한 기능은 고객이 설정할 수 없고 Edge DNS 플랫폼의 고유한 알고리즘에 의해 작동됩니다.

- **DNS 화이트리스트** - Akamai는 인터넷에서 정상적인 DNS 룩업의 약 95%를 담당하는 리커시브 리졸버의 행동에 대한 독자적인 가시성을 확보하고 있습니다. 과부하 상태에서 필요에 따라 Edge DNS는 포지티브 보안 모델을 사용하고 DNS 요청을 알려진 정상 DNS 리졸버 목록으로 제한할 수 있습니다.

용량

DDoS 제어는 DNS Flood의 영향을 줄이는 데 유용하지만, 다른 유형의 네트워크 계층 DDoS 공격에는 대량 트래픽을 흡수할 수 있는 충분한 네트워크 가용 용량이 필요합니다. 대형 공격의 리스크는 지난 몇 년 동안 크게 증가했으며, 알려진 가장 큰 규모의 공격은 현재 최대 대역폭이 1Tbps를 훨씬 초과합니다.

Akamai는 공격자에게 정량화할 수 있는 표적을 알려주지 않기 위해 Edge DNS 플랫폼의 용량을 공개하지 않습니다. 하지만 Akamai는 플랫폼 확장성의 모든 측면에 지속적으로 투자하여 새로운 고객과 인터넷의 트래픽 성장에 발맞춰 Edge DNS 인프라를 발전시키고 있습니다. Akamai는 클라우드 서비스 사업자로서 서버의 용도를 신속하게 변경하고 새로운 지역에 DNS 용량을 배포할 수 있습니다. Akamai는 대량으로 급증하는 트래픽을 흡수할 수 있는 상당한 규모의 가용 용량을 유지하고 있으며, 보통 Edge DNS 플랫폼은 전체 용량의 1% 미만을 소비합니다. 필요한 경우 Edge DNS는 다른 Akamai 플랫폼의 리소스를 활용하여 DDoS 공격을 완화할 수도 있습니다.

다른 Akamai 플랫폼 활용

네트워크 용량을 기반으로 고대역폭 DDoS 공격을 방어하는 능력을 측정하는 기존의 방법은 Edge DNS에는 적용되지 않습니다. Edge DNS는 다른 Akamai 플랫폼의 리소스를 활용할 수 있기 때문입니다. Akamai는 DNS 기업에 국한되지 않습니다. Edge DNS 이외에 다른 많은 서비스를 운영하고 있습니다. Akamai가 운영하는 모든 서비스 중 권한 DNS는 다른 서비스의 운영에 매우 중요하지만 전체 트래픽 측면에서 차지하는 비중은 작습니다. 따라서 필요한 경우 Edge DNS가 사용할 수 있는 용량을 늘릴 수 있습니다.

- **CDN에서 용량 빌려오기** - 대부분의 경우 Edge DNS는 Akamai CDN에서 실행되는 다른 Akamai 서비스에 속하는 서버와 동일한 PoP 내에 네임 서버를 배포합니다. 이러한 PoP는 훨씬 더 높은 대역폭을 사용하는 서비스를 지원하도록 설계되었기 때문에 용량이 훨씬 더 큰 경우가 많습니다. 따라서 Akamai는 필요한 경우 기타 서비스를 다른 Akamai PoP를 통해 이동시키고 공유된 네트워크 용량을 Edge DNS 전용으로 만들 수 있습니다. 이를 통해 대규모 DDoS 공격을 흡수할 수 있고 CDN에서 용량을 빌려오는 운영의 탄력성을 갖게 됩니다.
- **전용 방어 역량 구축** - Akamai는 권한 DNS 및 CDN 외에도 전용 방어 역량 및 기능을 갖춘 별도의 DDoS 방어 서비스를 운영합니다. 대규모 DDoS 공격을 방어하기 위해 필요한 경우 Akamai는 Prolexic 스크러빙 센터를 통해 개별 네임 서버 위임을 할당하여 전용 용량 및 DDoS 방어 툴을 활용할 수 있습니다. 이를 통해 Prolexic 플랫폼의 DDoS 방어 역량을 Edge DNS에 효과적으로 배포하여 Edge DNS의 리소스를 보존함으로써 최종 사용자의 정상적인 쿼리에 응답합니다.

다수의 DNS 벤더

Edge DNS는 여러 경쟁사 서비스보다 몇 배 더 큰 용량, 세그먼트된 수많은 IP Anycast 클라우드를 보유한 안정적인 아키텍처, 추가 용량을 활용할 수 있는 능력, DDoS 공격으로부터 기타 Akamai 서비스를 보호하는 역량을 갖춘 권한 DNS 서비스를 제공합니다. 이러한 장점을 바탕으로 고객의 유일한 권한 DNS 사업자로서 운영에 필요한 가용성과 안정성을 제공할 수 있습니다. 하지만 기존 솔루션과 Edge DNS를 같이 사용할 수도 있습니다. 멀티벤더 구축을 통해 기업은 기존 DNS 레코드 관리 방식을 유지하면서 기본 DNS 솔루션을 보완하여 Edge DNS의 가용성 및 이중화 기능을 추가할 수 있습니다.

배포 옵션

Edge DNS는 멀티벤더 환경에 Edge DNS를 배포하기 위한 여러 가지 옵션을 지원합니다.

- **기존 솔루션 보완** - 이미 DNS 솔루션을 사용하고 있는 기업은 기존의 DNS 솔루션을 강화하기 위해 Edge DNS를 보조 서비스로 배포할 수 있습니다. 기존의 솔루션 제공업체를 통해 DNS 레코드를 계속 관리하고 존(zone) 전송 또는 Edge DNS API를 사용하여 Edge DNS를 자동으로 업데이트합니다. 기존 및 보조 솔루션 모두 추가적인 최종 사용자의 쿼리에 응답하기 때문에 가용성을 강화할 수 있습니다.
- **숨겨진 마스터** - Akamai는 내부 DNS 솔루션에서 DNS 레코드를 지속적으로 관리하려는 기업에게 이 배포 옵션을 권장합니다. Edge DNS(유일한 보조 DNS 공급업체 또는 여러 공급업체 중 하나)는 숨겨진 마스터 옵션을 통해 내부 솔루션을 DDoS 공격에 노출시키지 않고 최종 사용자 쿼리에 응답할 수 있습니다. 기존의 솔루션 제공업체를 통해 DNS 레코드를 계속 관리하고 존(zone) 전송 또는 Edge DNS API를 사용하여 Edge DNS를 자동으로 업데이트합니다.
- **듀얼 기본** - 숨겨진 마스터 개념의 변형입니다. 일부 클라우드 서비스 공급업체는 더 이상 기존의 존 전송 기능을 사용하지 않으며, 존 레코드를 변경하려는 고객에게 API 또는 기타 사용자 인터페이스를 사용할 것을 요청합니다. Edge DNS는 기본 모드로 구성되고 Edge DNS 클라우드를 권한으로 추가하는 방식으로도 활용할 수 있습니다.

보조 DNS로서 가용성 유지

Edge DNS를 보조 DNS 솔루션으로 사용할 때 기본 DNS 솔루션의 존 업데이트를 통해 최종 사용자 쿼리에 올바르게 응답합니다. 일반적으로 존 파일은 SOA 레코드(Start of Authority record)의 만료 필드에 의해 제어되는 TTL(Time-To-Live)에 대한 보조 DNS 솔루션에서 유효한 상태로 유지됩니다. 기본 솔루션에 장애를 발생시키는 DDoS 공격은 중단 길이가 TTL 값을 초과하게 되면 보조 솔루션이 쿼리에 응답하지 않도록 할 수도 있습니다. Edge DNS는 TTL이 만료된 후에도 존 파일을 보유하며 DNS 레지스트리가 Edge DNS를 가리키는 동안 DNS 쿼리에 계속 응답하여 이 시나리오를 방어합니다. 이를 통해 기본 솔루션을 사용할 수 없는 경우에도 보조 DNS 솔루션으로 추가 가용성을 제공할 수 있습니다.

결론

현재 알려진 가장 큰 규모의 DDoS 공격은 최대 대역폭이 1Tbps를 초과합니다. 클라우드 기반 서비스의 사용 가능한 대역폭을 계산한다고 해서 이런 공격에 대응할 수 있는 안정성에 대한 정확한 정보를 찾을 수는 없습니다. 작은 규모의 공격도 특정 지역 내에서 장애를 일으킬 수 있습니다. Edge DNS는 가용성에 대한 멀티레이어 접근 방식을 통해 고객에게 100%의 가용성을 제공하며, 다음과 같은 기능을 포함합니다.

- 경쟁사 서비스에 비해 몇 배 더 큰 규모의 네임 서버 및 PoP를 비롯한 전 세계적인 범위의 대규모 확장성
- 공격의 영향을 격리하고 전체 플랫폼 뿐만 아니라 다른 고객이 입을 부수적인 피해를 방지하기 위해 세그먼트된 다수의 IP Anycast 클라우드를 갖춘 안정적인 아키텍처
- 필요에 따라 DDoS 제어를 배포하거나 고객 위임을 재할당할 수 있는 기능 등을 통해 DDoS 공격에 탄력적으로 대응
- Akamai CDN 및 Prolexic의 DDoS 방어 등 다른 Akamai 서비스를 활용하여 용량을 늘리고 대규모 및 소규모 DDoS 공격 방어

권한 DNS는 전 세계의 사용자를 기업의 온라인 시스템과 연결시키는 미션 크리티컬 서비스입니다. Edge DNS는 단독 권한 DNS 솔루션으로 배포되거나 또는 기존의 DNS 솔루션과 함께 배포되는 경우 모두 웹사이트 및 기타 인터넷 기반 애플리케이션에 대한 글로벌 접속을 유지하는 데 필요한 가용성을 기업에게 제공합니다.