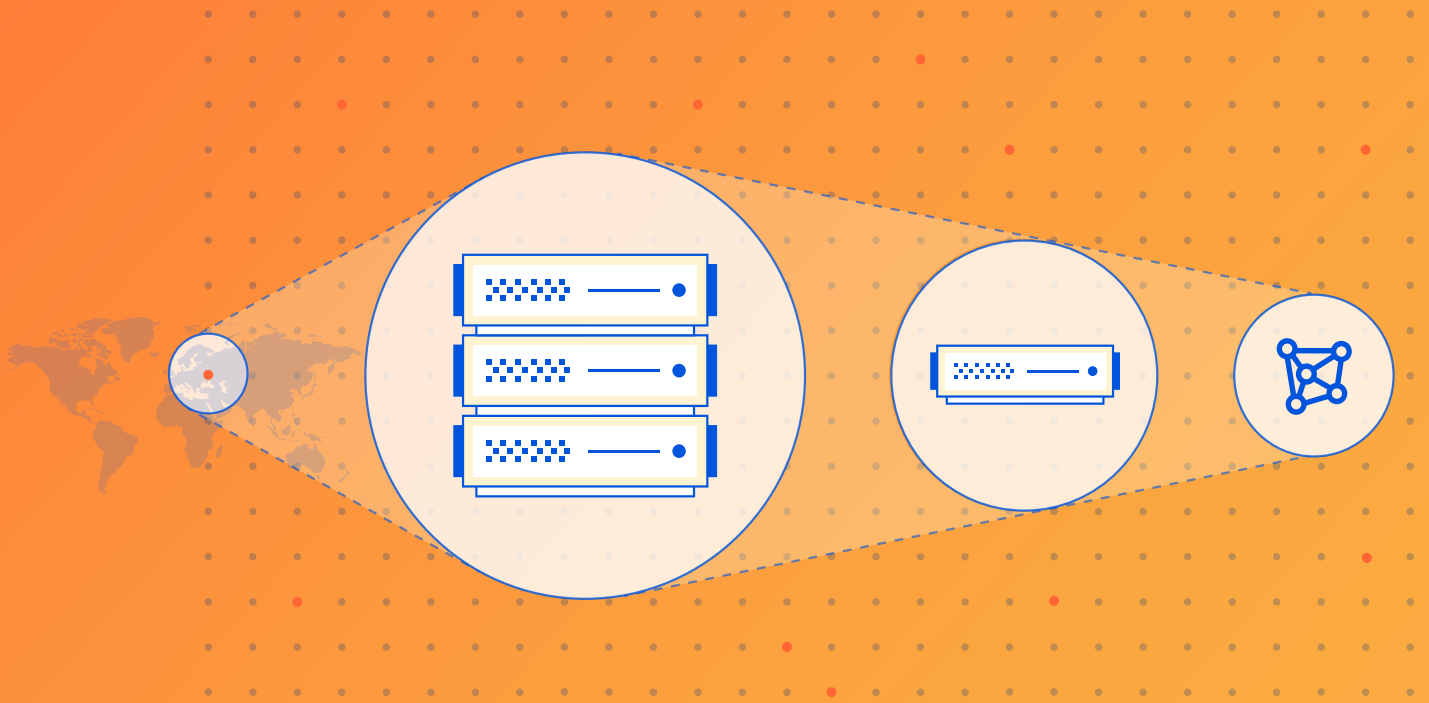
CLOUDFLARE

백서

DNS 및 DDoS 위협



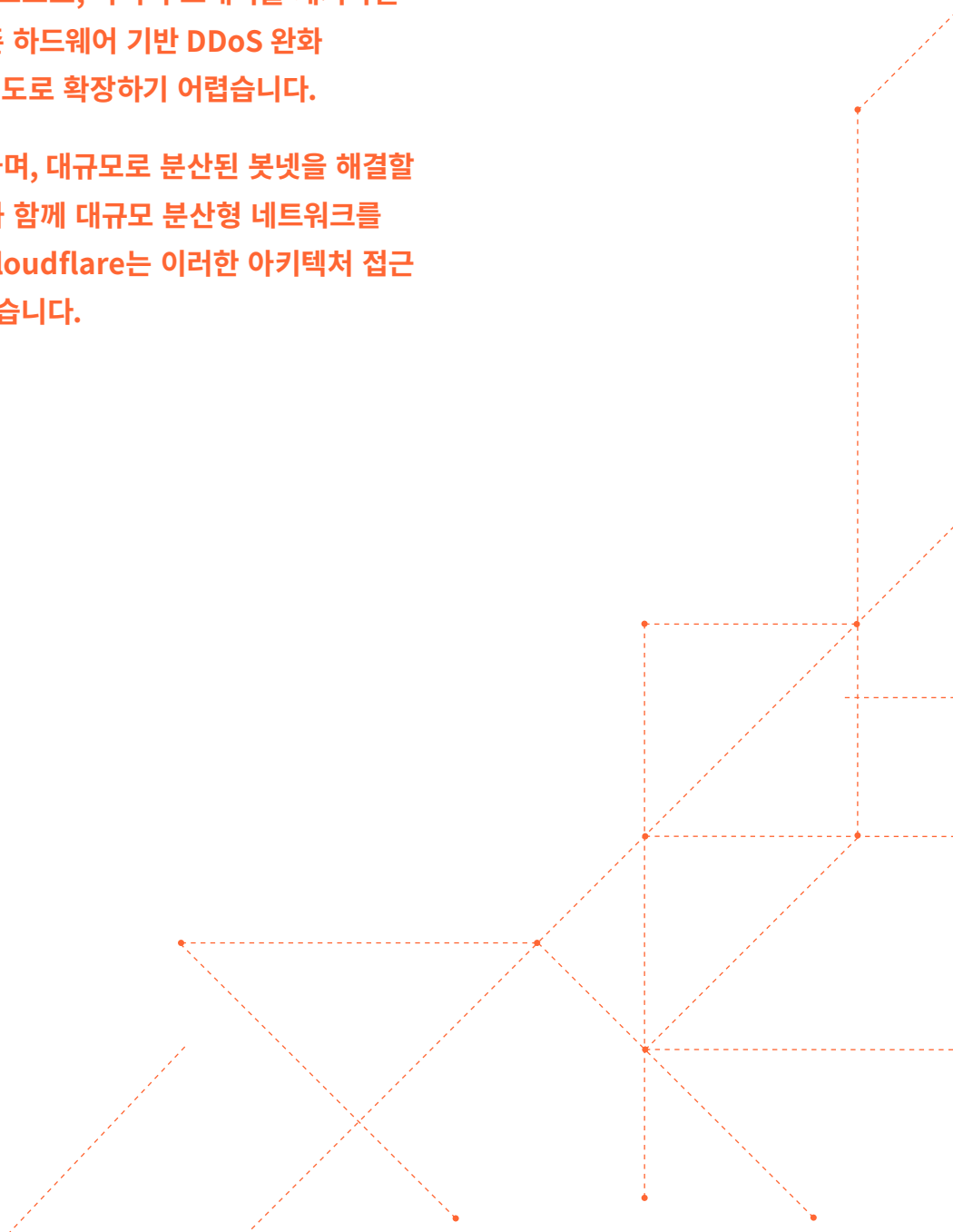
내용

핵심 요약

도메인 네임 시스템(DNS)은 인터넷을 실현한 주요 혁신 중 하나였습니다. 그러나 현재는 대규모 봇넷을 사용해 그 어느 때보다 규모가 큰 사이버 공격을 개시하는 데 DNS 인프라를 이용하고 있으며, DNS 인프라는 목표물이 되고 있습니다.

최근 공격자는 여러 중요한 사이트와 조직의 DNS에 대규모 분산 서비스 거부(DDoS) 공격을 수행해 필수 서비스와 다수 인터넷 영역을 공격해왔고, 이는 서비스 장애 및 중단으로 이어졌습니다. 봇넷은 기본적으로 무료이며 분산되어 있으므로, 악의적 트래픽을 제거하는 데 스크러빙 센터를 사용하는 기존 하드웨어 기반 DDoS 완화 서비스는 비용 측면에서 유리한 정도로 확장하기 어렵습니다.

Cloudflare는 아키텍처가 중요하며, 대규모로 분산된 봇넷을 해결할 유일한 솔루션은 보안 DNS 확인과 함께 대규모 분산형 네트워크를 사용하는 것이라고 생각합니다. Cloudflare는 이러한 아키텍처 접근 방식을 기반으로 서비스를 만들었습니다.



늘어나는 대규모 공격이 DNS에 새로운 수준의 위협을 가져오다

2016년 10월 21일, 지속적인 대규모 분산 서비스 거부(DDoS) 공격이 인터넷의 막대한 부분에 영향을 줬습니다. 이로 인해 수십 개의 중요한 웹 사이트와 서비스가 장애를 경험하거나 중단되었습니다. 이 공격의 직접적인 목표물은 DNS 서비스 공급자인 Dyn이었습니다. 이 공급자는 도메인 이름을 자사 인터넷 프로토콜(IP) 주소에 매핑하여 특정 사이트로 트래픽을 라우팅합니다. 이 공격을 완화하는 데는 몇 시간이 소요되었습니다.[1]

하지만 상당한 규모의 DDoS 공격은 끝이 아니었습니다. 이후 수년간 공격의 규모와 범위가 늘어났으며 기록적인 규모의 사이버 공격이 정점에 달했습니다. AWS는 2020년 2월에 대규모 DDoS 공격을 완화했다고 보고했습니다. 공격이 가장 심각했을 때는 초당 2.3테라비트(Tbps)의 속도로 트래픽이 수신되었습니다.[2] Cloudflare는 2022년 6월에 초당 2천 6백만 개 요청에 달하는 DDoS 공격을 완화했습니다. 그때까지 발생한 HTTPS DDoS 공격 중 가장 큰 규모였습니다.[3]

공격자는 어떻게 이 정도로 공격을 확장할까요?

IoT 기반 및 서버 기반 대규모 봇넷

대규모 공격을 개시하는 주요 방법의 하나는 보안이 취약한 사물 인터넷(IoT) 장치를 탈취하는 것입니다. Mirai 봇넷은 악의적인 목적으로 악용한 IoT 장치 네트워크에서 가장 대표적인 예시라고 할 수 있습니다. Mirai 생성자는 가정용 라우터, 스마트홈 장치, 보안 카메라, 비디오 레코더 등 연결되어 있는 장치 100,000개 이상을 손상시켜 거대한 봇넷을 생성했고, 잠재적으로 최대 1.2Tbps의 트래픽을 발생시키는 Dyn 공격 등을 개시하는 데 이용했습니다.

이 대규모 봇넷은 Dyn을 압도했고, Dyn을 이용하는 모든 웹 사이트와 애플리케이션의 DNS 확인이 중단되었습니다.

> **"장치에 공개적으로 액세스할 수 있다고 가정하면 해킹을 당할 확률은 아마 100%일 것입니다. IPv4 주소 공간은 그렇게 크지 않습니다. 특히 큰 봇넷이 있는 경우, 전체 공간을 몇 시간이면 스캔할 수 있습니다. 취약성에 대한 스캔은 지속해서 진행되고 있으며, 오히려 지난 몇 년 동안 더욱 가속화되었습니다."**
>
> - Matthew Prince, Cloudflare CEO

이 봇넷은 Mirai라는 맬웨어를 사용하여 만들어졌습니다. Mirai는 공장 기본 설정인 사용자 이름과 비밀번호 설정을 그대로 사용하는 장치를 인터넷에서 찾아 손쉽게 감염시키고 로그인하여 장치를 탈취할 수 있습니다. 장치 소유자는 가끔 성능이 느려졌다는 것 외에는 장치가 손상되었다는 사실을 알아차리지 못합니다.

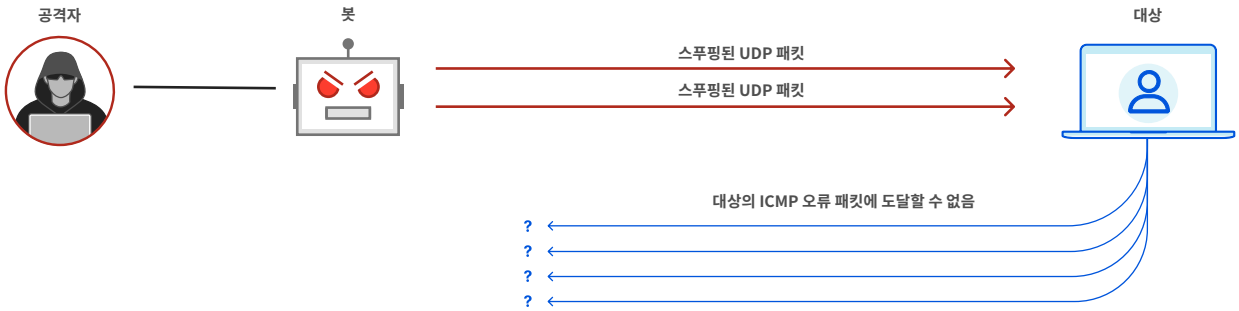
현재도 Mirai 봇넷은 여전히 위협적이지만, 이 봇넷만 DDoS 공격에 자주 사용되는 것은 아닙니다.

- **Meris 봇넷**은 2021년 6월에 처음 감지되었습니다. 연구자들은 이 봇넷에서 봇을 30,000개 이상 찾았지만, 실제 봇 수는 훨씬 많을 것이라 예상되고 있습니다.[4]
- **Mantis 봇넷**은 IoT 장치 대신, 탈취한 가상 머신과 강력한 서버를 사용합니다. 즉, 각각의 봇에 Mirai 봇넷이나 Meris 봇넷의 장치보다 컴퓨팅 리소스가 더 많습니다. 경우에 따라 이 봇넷은 초당 2천 6백만 개의 요청에 달하는 대규모 DDoS 공격을 개시할 수 있습니다.[5]

DNS 작동 방식을 악용하는 방식 중 가장 일반적인 두 가지는 DNS 증폭(또는 '반사') 및 UDP 폭주 공격입니다.

DNS 서버 압도: UDP 폭주

UDP 폭주 공격은 장치가 처리하고 응답할 수 있는 능력을 압도하기 위해 UDP 패킷을 대상 서버로 다수 전송합니다. UDP 폭주로 인해 목표 서버를 보호하는 방화벽까지 성능이 떨어져, 합법적인 트래픽에 서비스를 거부하게 됩니다.



이러한 공격은 특히 DNS 확인자와 관련되어 있습니다. 일반적으로 모든 DNS 트래픽이 UDP를 통해 전송되기 때문입니다(영역 전송과 같이 일부 특수 사용 사례에서만 TCP가 사용됨). UDP는 연결을 시작하는 데 핸드셰이크가 필요하지 않으므로 쓸모없는 UDP 패킷을 목표물에 대량으로 전송할 수 있으며, 목표물은 최선을 다해 각 패킷에 응답합니다. (예를 들어 Dyn에 수행된 Mirai 공격은 UDP 폭주 공격이었습니다. DNS를 겨냥한 공격이라면 'DNS 폭주'라 부릅니다.)

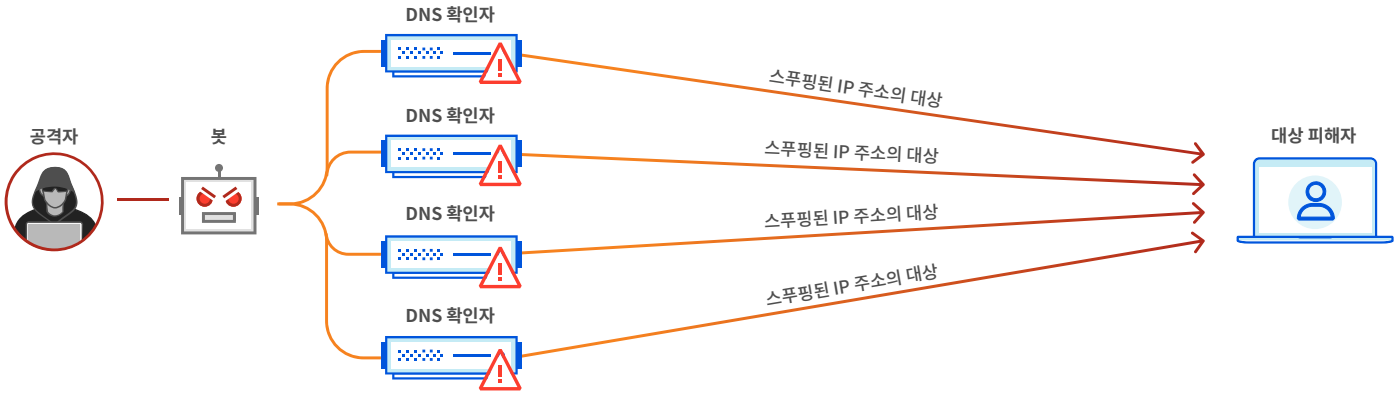
UDP 폭주는 기본적으로 서버의 한 포트에 UDP 패킷이 전송되었을 때 수행되는 단계를 악용하여 작동합니다. 이 포트에 패킷을 수신하는 프로그램이 없다면, 서버는 대상에 도달할 수 없음을 알리기 위해 ICMP(ping) 패킷으로 발신자에게 응답합니다. 서버가 각각의 새로운 UDP 패킷을 수신하고 있으므로, 패킷은 요청 처리 단계를 거치며 이 과정의 서버 리소스를 활용합니다. 목표물이 된 서버가 수신한 각 UDP 패킷을 확인한 다음에 응답하기 위해 리소스를 활용하므로 UDP 패킷을 대량으로 수신한다면 목표 서버의 리소스는 빠르게 소진됩니다.

DNS 작동 방식 악용: DNS 증폭

목표 DNS 서비스 공급자를 바로 공격하는 것 외에도, 공격자는 이 인프라를 무기로 활용하고 DNS의 작동 방식을 이용해 다른 목표물에 치명적인 DDoS 공격을 수행할 수도 있습니다.

DNS 증폭 공격은 열린 DNS 확인자의 기능을 활용하여 증폭시킨 트래픽 양으로 목표 서버나 네트워크를 압도합니다. 피해자를 직접 공격하는 대신, 공격의 각 봇은 목표한 피해자의 실제 소스 IP 주소로 변경하여 스푸핑한 IP 주소로 열린 DNS 확인자에 요청을 전송합니다. 그러면 목표물이 DNS 확인자로부터 응답을 받게 됩니다.

공격자는 DNS 확인자가 최대한 크게 응답을 생성하도록 요청을 구성합니다. 이렇게 하면 목표물이 공격자의 최초 트래픽을 증폭하여 수신합니다. CISA(사이버 보안 및 인프라 보안국)의 추정에 따르면, DNS 증폭 공격을 이용하는 공격자는 스푸핑하여 전송한 패킷 대역폭의 54배까지 트래픽을 증폭해 전송할 수 있습니다.[6]



DNS 증폭은 Spamhaus에 수행되어 오프라인 상태를 만들었던 2013년의 공격에서 중요한 역할이었고,[7] 그밖의 다양한 공격에서 사용됐습니다.

공격의 직접적인 원인이 DNS 확인자인 것은 아니지만, 예방할 수 있는 시스템 악용이며 예방해야만 합니다. 자체 호스팅 DNS를 사용하는 조직의 경우 이러한 시스템을 악용해 내부 네트워크가 중단될 수도 있습니다.

대규모 DDoS 공격이 DNS 확인자 및 다운스트림 피해자에 미치는 영향

DDoS 공격을 경험한 조직은 부정적인 영향이 광범위하다는 점을 인식하게 되었습니다. 이러한 영향으로는 가동 중단 시간, 비즈니스 손실, 평판 저하, 큰 재무적 부담이 있습니다. DDoS 공격으로 인한 총 비용은 대기업의 경우 평균 2백만 달러, 중소기업의 경우 120,000달러라는 주장도 있습니다. 기업에서 DDoS 공격에 대응하는 데 드는 비용은 230만 달러에 달할 수 있습니다(2017년 계산 기준).[8]

DNS 공급자를 직접적으로 공격하면 해당 공급자를 이용하는 조직에도, 공급자에도 훨씬 심각한 영향을 미칠 수 있습니다. DNS가 중단된다면 조직은 새로운 공급자를 찾아야 할 수도 있습니다.

웹 사이트와 애플리케이션만이 DDoS 공격의 대상이 되는 것은 아닙니다. 온프레미스 네트워크를 겨냥하는 공격자도 있습니다. 공격이 진행되는 동안 자체 호스팅 DNS를 사용하는 조직에서는 장애를 경험하게 되므로, 클라이언트 장치가 필요한 리소스를 가져올 수 없게 될 수 있습니다. 이러한 공격은 조직의 운영에 큰 지장을 주거나 운영을 전부 중단시킬 수도 있습니다.

DNS 인프라를 겨냥하여 다가오는 위협을 막을 방법

결국 잘 만들어진 아키텍처만이 매년 규모가 늘어나는 DDoS 공격을 막을 수 있습니다.

하드웨어를 통한 기존의 DDoS 완화와 소프트웨어를 통한 확장 가능한 완화 비교

공격을 차단하는 기존의 방법은 커다란 하드웨어를 구매하거나 구축하여, 유입되는 트래픽을 필터링하는 것이었습니다. 기존 DDoS 완화 서비스 공급업체 대부분은 Cisco, Arbor Networks, Radware와 같은 회사의 하드웨어를 함께 사용하여 '스크러빙 센터'를 구축했습니다.

이렇게 거대한 완화 하드웨어를 함께 작동시키는 방편들이 있긴 했지만 불편했습니다. 단일 하드웨어가 흡수할 수 있는 패킷 수에 물리적인 제약이 있었고, 이 제약은 서비스 공급자가 완화할 수 있는 총용량의 효과적 한계가 되었습니다. 아주 큰 규모의 DDoS 공격 상황에서는 업스트림 ISP가 병목현상을 일으키는 위치가 아주 적어, 대부분의 공격 트래픽은 절대 스크러빙 센터에 도달하지 않았습니다.

장비 비용은 스크러빙 하드웨어를 광범위하게 배포하는 것이 비용 효율적이지 않다는 것을 보여주었습니다. 레거시 DDoS 공급업체는 고객이 공격받고 있을 때만 서비스를 프로비저닝하는 것이 일반적이었습니다. 그러나 이전에 수행된 가장 큰 공격보다 일정 수준 이상 용량을 확보하는 것은 결코 이치에 맞지 않습니다.

그 이상 투자하면 낭비라고 가정하는 게 합리적인 것 같았습니다. 그러나 결국, 이러한 가정은 이 전통적인 모델에 치명적이었습니다.

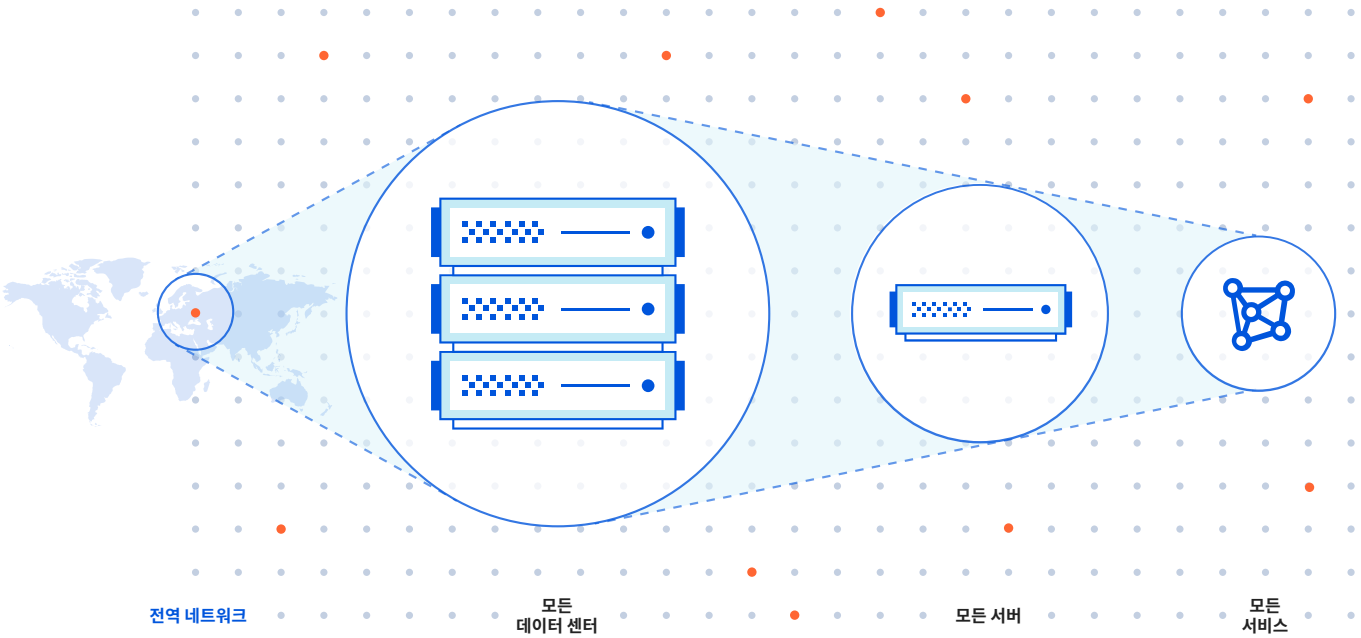
하드웨어는 미래가 아니다

Cloudflare는 DDoS 완화용 하드웨어에 투자하는 대신, 처음부터 아주 단순한 아키텍처로 시작했습니다. Cloudflare의 첫 번째 랙에는 라우터, 스위치, 서버 세 가지 구성 요소만이 있었습니다. 오늘날 랙은 더 단순해졌으며, 종종 라우터를 완전히 없애고 데이터 센터가 서비스하는 지리적 영역에 걸쳐 패킷을 라우팅할 수 있도록 라우팅 테이블도 충분히 처리할 수 있는 스위치를 사용합니다.

Cloudflare는 공격 시 병목 현상이 일어날 수 있는 로드 밸런서나 전용 완화 하드웨어를 사용하는 대신, 인터넷의 기본 라우팅 프로토콜인 경계 경로 프로토콜(BGP)을 활용하여 지리적으로 로드를 분산하며 네트워크 내 각 데이터 센터 내에서 로드를 분산하는 소프트웨어를 만들었습니다. 모든 랙의 모든 서버는 모든 유형의 요청에 응답할 수 있습니다. Cloudflare 소프트웨어는 특정 시점에 특정 고객에게 필요한 만큼 트래픽 로드를 동적으로 할당합니다. 즉, 대규모 공격이 이루어질 때 Cloudflare는 말 그대로 수만 개의 서버에 걸쳐 로드를 자동으로 분산시킵니다.

그래서 Cloudflare는 네트워크에 계속 비용 효율적으로 투자할 수 있습니다. 예를 들어, 어떤 도시에 용량이 10% 더 필요하다면 Cloudflare는 스크러빙 하드웨어를 더 구매하거나 구축하기 위해 계단함수 결정을 내리는 대신 10%의 용량을 추가적으로 전송할 수 있습니다.

모든 코어와 모든 서버, 모든 데이터 센터에서 공격을 완화하도록 도움을 줄 수 있으므로, Cloudflare가 온라인으로 제공하는 각각의 새로운 데이터 센터는 서비스를 개선하고 소스에서 더 가까운 공격을 차단할 수 있도록 합니다. 달리 말하면, 대규모 분산형 봇넷에 대한 솔루션은 대규모 분산형 네트워크라는 것입니다. 이것이 바로 소수의 스크러빙 위치에서 역량을 집중하는 것이 아니라 힘을 분산함으로써 인터넷이 작동하는 방식입니다.



Cloudflare가 쉽게 DNS 보안을 확장하는 방법

Cloudflare는 분산형 네트워크를 사용하여 악의적인 트래픽을 효율적으로 차단하고 흡수할 뿐만 아니라 모든 위치에서 권한 있는 DNS 및 DNS 확인을 제공합니다. 모든 데이터 센터에서 DNS 응답을 제공하므로 DNS 쿼리는 최소한의 대기 시간으로 해결됩니다. 또, Cloudflare의 DNS는 전체 네트워크의 용량을 이용하고 분산된 특성의 이점을 누릴 수 있습니다.

Cloudflare 네트워크는 리소스를 효율적으로 사용하므로 운영 비용과 자본 비용까지 절약됩니다. Cloudflare는 동일한 장비와 네트워크를 사용하여 모든 기능을 제공하기 때문에 Cloudflare가 공격 차단이나 기타 모든 서비스를 제공하는 데 관련되는 추가 대역폭 비용은 거의 없습니다.

Cloudflare의 기능이 지속해서 확장되면 이에 비례해 공격 차단 역량도 늘어납니다. Cloudflare는 공격의 규모와 관계없이 고정 가격의 DDoS 완화 서비스를 고객에게 제공할 수 있습니다. 공격으로 인해 Cloudflare의 단위 비용이 가장 크게 증가되지는 않기 때문입니다.

모두 동일한 역량을 가진 방대한 분산형 서버 네트워크는 방대한 규모와 최소한의 대기 시간으로 Cloudflare가 다양한 기능까지 수월하게 제공할 수 있습니다. 가장 핵심적인 서비스로는 권한 있는 보조 DNS가 있습니다. Cloudflare는 세상에서 가장 빠른 DNS 확인자입니다.[9]

Cloudflare 전역 Anycast 네트워크를 통해 275개 이상의 도시에 있는 데이터 센터 각각의 네트워크 에지에서 DNS를 확인하므로, 최고의 이중화와 100% 가동 시간을 제공합니다. Cloudflare 네트워크 용량으로 DDoS 공격을 충분히 흡수할 수 있으므로, DNS는 모든 규모와 유형의 공격에 대응할 정도로 복원력을 갖출 수 있습니다.

군비 경쟁에서 승리를 거두고 DDoS 공격에 대항할 복원력 유지하기

- 2022년 4분기 Cloudflare 네트워크 용량: **172Tbps**(늘어나고 있음)
- 역대 최대 규모의 DDoS 공격: **2.5Tbps 미만**

DDoS 공격의 규모는 앞으로도 계속 기하급수적으로 커질 수 있습니다. 하지만 Cloudflare는 미래에 다가올 군비 경쟁에서 계속 승리하기 위해 준비되어 있습니다.

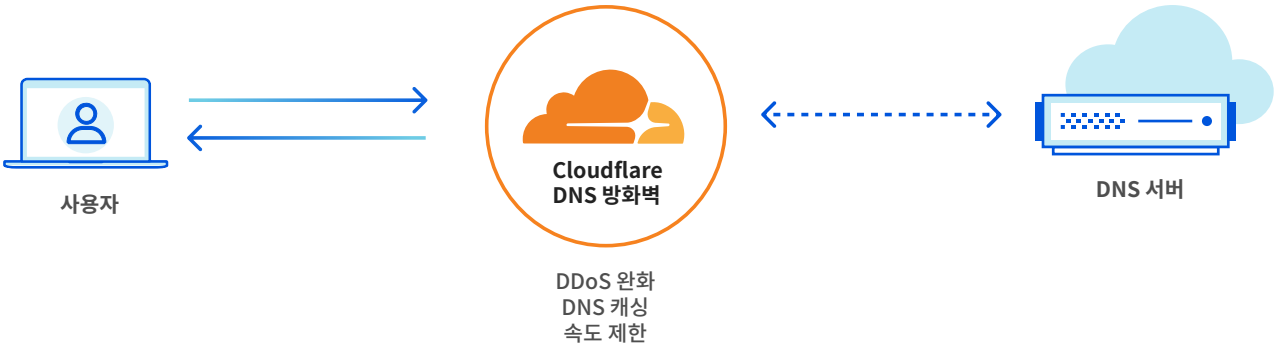
Cloudflare는 처음부터 대규모 DDoS 공격을 완화하도록 설계된 유일한 공급자입니다. DDoS 공격이 본질적으로 분산된 것처럼 Cloudflare의 DDoS 완화 시스템 역시 대규모의 전역 네트워크에 분산되어 있습니다.

공격자는 대부분의 레거시 서비스 공급자보다 유리합니다. 공급자는 값비싼 하드웨어와 대역폭을 구매해야 하므로 비용이 많이 들지만, 공격자는 압도적으로 많은 해킹된 장치를 사용하며 목표물에 비대칭적인 양의 트래픽을 생성하기 때문에 비용이 많이 들지 않습니다. 그렇기 때문에, Cloudflare의 대규모 분산형 상용 하드웨어 네트워크에 로드를 할당하는 소프트웨어가 바로 Cloudflare의 비결입니다.

모든 종류의 공격과 악용으로부터 DNS 보호하기

2022년 4분기 기준, Cloudflare는 초당 약 2천 260만 개의 DNS 쿼리(권한 있는 요청 및 확인 요청 모두 포함)를 처리합니다. 늘어나는 DDoS 공격까지 동시에 완화하고 있습니다. 오늘날의 대규모 DDoS 공격부터 DNS 물고문 및 기타 남용까지, Cloudflare DNS는 모든 규모의 DDoS 및 봇 공격에 대한 복원력을 유지하고 있습니다.

Cloudflare DNS 방화벽은 자체 DNS 인프라를 호스팅하는 DNS 서비스 공급자와 조직이 대규모 DDoS 공격으로부터 인프라와 사용자를 보호하도록 지원하면서도, DNS 레코드를 캐시하고 대신 응답하여 성능을 개선합니다.



Cloudflare DNS 및 DNS 방화벽 솔루션에는 기본적으로 DDoS 완화가 포함되어 있으므로, 역사상 가장 큰 규모의 DDoS 공격을 받을 때에도 애플리케이션은 항상 보호되며 언제나 작동합니다.

요점

Cloudflare는 계속 확장하고 있으며, 주기적으로 도시와 국가를 더 많이 네트워크에 추가하고 있습니다. 언제나 Cloudflare는 새로운 공격을 경계하고 있지만, Cloudflare의 아키텍처야말로 궁극적으로 앞으로 나타날 공격을 차단할 수 있는 올바른 방법이라고 자신합니다. DNS를 겨냥한 공격을 현재와 미래에 모두 차단하기 위해 구축된 네트워크와 협업해보세요.

- Cloudflare를 설정하여 봇넷 기반 DDoS 공격과 증폭 공격 등 모든 DDoS 공격으로부터 보호를 받으세요
- 권한 있는 DNS 공급자의 역할을 Cloudflare에 맡겨 공격을 받는 도중에도 DNS를 유지하고 실행하세요
- Cloudflare DNS 방화벽으로 속도를 제한하고 공격을 차단하여 DNS 인프라와 잠재적 DDoS 피해자를 보호하세요

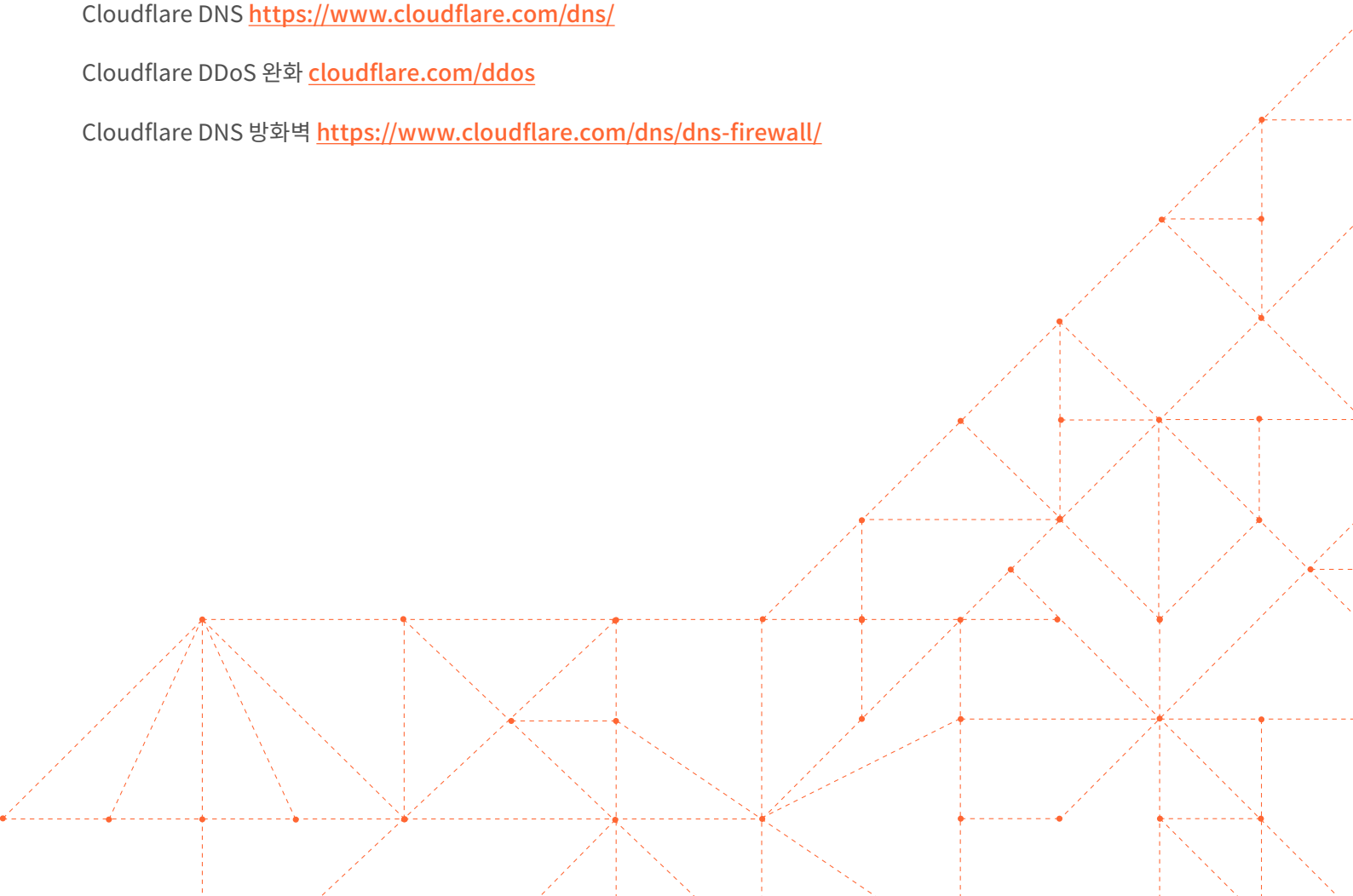
설정은 매우 간단하며, 시작부터 실행까지 5분도 걸리지 않습니다. Free부터 Enterprise까지 다양한 요금제를 cloudflare.com/plans에서 확인해 보세요.

Cloudflare 솔루션에 대해 자세히 알아보려면 다음 사이트를 방문하세요.

Cloudflare DNS https://www.cloudflare.com/dns/

Cloudflare DDoS 완화 cloudflare.com/ddos

Cloudflare DNS 방화벽 https://www.cloudflare.com/dns/dns-firewall/



참고자료

1. “DDoS Attack Against Dyn Managed DNS.” Dyn Statue Updates, 2016년 10월 21일, https://www.dynstatus.com/incidents/nlr4yrr162t8. 2022년 10월 3일 액세스.
2. Cimpanu, Catalin. “AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever.” ZDNET, 2020년 6월 17일, https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/. 2022년 10월 3일 액세스.
3. Yoachimik, Omer. “Cloudflare mitigates 26 million request per second DDoS attack.” Cloudflare, 2022년 6월 14일, https://blog.cloudflare.com/ko-kr/26m-rps-ddos-ko-kr/. 2022년 10월 3일 액세스.
4. Ganti, Vivek and Omer Yoachimik. “A Brief History of the Meris Botnet.” Cloudflare, 2021년 11월 9일, https://blog.cloudflare.com/meris-botnet/. 2022년 10월 3일 액세스.
5. Yoachimik, Omer. “Mantis - the most powerful botnet to date.” Cloudflare, 2022년 7월 14일, https://blog.cloudflare.com/mantis-botnet/. 2022년 10월 3일 액세스.
6. “Alert (TA14-017A): UDP-Based Amplification Attacks.” CISA, 2019년 12월 18일, https://www.cisa.gov/uscert/ncas/alerts/TA14-017A. 2022년 10월 24일 액세스.
7. Prince, Matthew. “The DDoS That Knocked Spamhaus Offline (And How We Mitigated It).” 2013년 3월 20일, https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/. 2022년 10월 24일 액세스.
8. Kobialka, Dan. “Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Totals $2M.” MSSP Alert, 2018년 2월 25일, https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/. 2022년 10월 3일 액세스.
9. “DNS Performance Analytics and Comparison.” DNSPerf, https://www.dnsperf.com/. 2022년 10월 24일 액세스.

CLOUDFLARE

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/3855.20221104