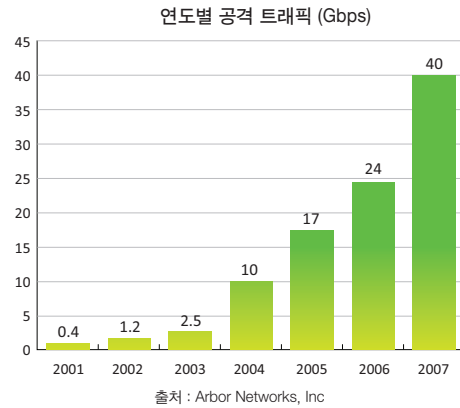


Secured Hosting

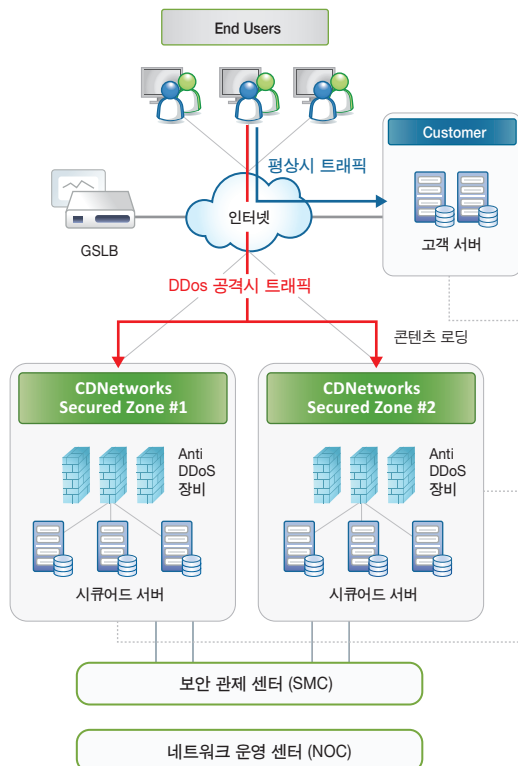
개요

2009년 7월 7일 발생한 DDoS 대란으로 인해 대규모 인프라를 자랑하는 포털이나 커뮤니티, 일부 정부기관까지 DDoS 공격을 받아 수 일째 정상적인 서비스를 제공하지 못했던 사례에서 드러나듯이, 예전 일부 특정 사이트에 대해서만 행해지던 DDoS 공격이 최근에는 사업자 규모, 업종을 가릴 것 없이 무차별적으로 이뤄지면서 그 피해 규모는 날로 커지고 있습니다. 게다가 최근에는 기존의 수 Gbps의 대량 트래픽을 발송해 네트워크 대역폭을 가득 차게 해 버리는 대역폭 공격뿐만 아니라 트래픽은 거의 유발하지 않으면서도 정상적인 웹 접속과 유사하게 웹과 DB 서버의 과부하를 유발하는 'HTTP Get Flooding 공격' 등 다양한 공격이 이루어지고 있습니다. 국내 수십 개의 Anti-DDoS 장비 업체와 DDoS 방어 전문 사업자들이 있지만 이러한 극한의 공격에도 서비스 지속을 보장할 수 있는 업체는 없습니다. 씨디네트웍스의 Secured Hosting 서비스는 트래픽 우회 기술과 대규모 시큐어드 서버에 기반한 방어 기술을 활용하여, 기존 DDoS 방어 시스템의 한계를 극복한 독보적인 서비스입니다. 국내와 아시아 1위, 전 세계 3위 CDN(콘텐츠 전송 네트워크)사업자로서의 역량을 활용한 서비스로서 고객 DDoS 방어 역량을 비약적으로 향상시킵니다.



구성도

DDoS 공격으로 인해 고객 시스템의 지속적인 서비스가 불가할 시에는 씨디네트웍스 GSLB에 의해 모든 트래픽을 씨디네트웍스 Secured Zone으로 우회합니다. 우회된 트래픽은 대규모 Anti-DDoS 장비와 시큐어드 서버에 의해 원활히 서비스합니다.



■ 정상 시 트래픽 처리

- 정상 시에는 고객 시스템으로 트래픽이 유입되어 처리됩니다. 고객 서버와 씨디네트웍스 시큐어드 서버 간에는 미리 주기적으로 콘텐츠를 일치 시킵니다.

■ 공격 시 트래픽 우회

- DDoS 공격 시에는 고객이 구축한 Anti-DDoS 시스템에서 우선적으로 방어합니다. 방어가 역부족일 경우, 모든 트래픽을 씨디네트웍스의 검증된 GSLB에 의해 Secured Zone으로 우회 시킵니다.
- GSLB(Global Server Load Balancer) : CDN 사업에 필수적인 시스템으로서 ISP/IDC간 트래픽 분산과 Fail-over를 제공합니다. 씨디네트웍스는 국내/아시아 1위 CDN 사업자로서 고도화된 GSLB 기능을 보장합니다.

■ 공격 시 트래픽 처리

- Secured Zone은 지리적으로 분산된 2개의 IDC에 대규모 Anti-DDoS 장비와 시큐어드 서버로 구성되어 있으며 우회된 트래픽을 처리합니다.
- Secured Zone : 대규모 Anti-DDoS 장비가 구축되어 있습니다. 또한, 고객의 원본 서버 콘텐츠를 미리 로딩한 시큐어드 서버는 트래픽에 탄력적으로 구성할 수 있어서 아무리 많은 공격 트래픽이 유입되어도 원활한 처리를 보장합니다.

특장점

기존 DDoS 방어 한계를 극복한 CDN 기반 방어 서비스로서, 트래픽 우회 처리, 대규모 인프라 기반 방어, 24x365 보안 관제의 특장점이 있으며, GSLB나 시큐어드 서버 등의 검증된 써드네트웍스의 인프라를 활용하여 완벽한 방어를 약속합니다.

DDoS 공격 트래픽 우회 처리 서비스

- **보험성 서비스** : 시스템 구축이나 이전의 필요 없이 계약만으로 즉시 서비스 가능하며 기존 고객의 DDoS 방어 역량을 획기적으로 증가 시킴
 - Anti-DDoS 시스템 자체 구축의 한계 극복 (한정된 시스템과 회선 용량)
 - Anti-DDoS 존 입주의 한계 극복 (고객 시스템의 IDC 이전이 필요하고 이전 후, IDC사업자의 비즈니스에 종속됨)
- **고객 콘텐츠 보안** : 고객 원본 서버와 주기적으로 콘텐츠를 일치시키는 시큐어드 서버는 고객 전용으로 할당되어 콘텐츠가 보호됨

대규모 인프라에 의한 완벽한 방어 서비스

- **Multi ISP 수용** : 공격 PC들이 단일 ISP에 집중될 경우 대비, 복수ISP 기반 서비스
- **40G 회선 대역폭** : 10G 4회선(40Gbps)으로 대규모 대역폭 고갈형 공격 방어 보장
- **분산 Secured Zone** : 지리적으로 분산된 Secured Zone 구성으로 서비스 지속성 보장
- **대규모 Anti-DDoS 장비** : 다수의 최신 Anti-DDoS 장비 구성으로 다양한 DDoS 공격 방어 보장
- **대규모 시큐어드 서버** : 유입 트래픽에 따라 탄력적으로 서버 구성하여 빠른 응답속도 보장

24 x 365 2중 보안 관제 서비스

보안 관제 센터 (SMC)

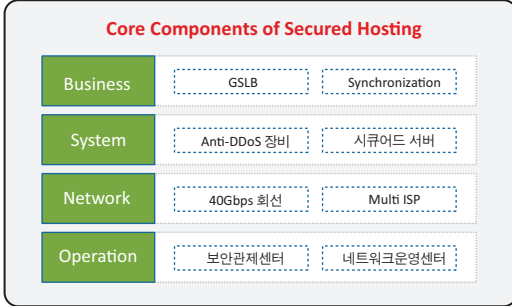
네트워크 운영 센터 (NOC)

Router: all	0.00	(0.00)	Out	2.53K	(0.00)	In
ICMP	40274	24K	(110.00)	Out	10220	24K
TCP	7.83K	(0.00)	Out	25.15K	(0.00)	In
UDP	-0.00K	(+0.00)	Out	0.00K	(0.00)	In
Other protocols						

- **2중 보안 관제** : 공격 모니터링, 인지, 대응, 전파의 관제 프로세스 준수하며 탐지와 대응을 바로 연계할 수 있는 명품 관제 제공
 - 보안관제센터(SMC) : DDoS 공격 관제
 - 네트워크 운영 센터(NOC) : 시스템 및 네트워크 관제
- **다수 관제 인력 운용** : 다수의 인력 기반 대응이 필수적인 세션 고갈형과 자원 고갈형 공격을 효과적으로 방어할 수 있도록 전문 인력 운용

기대효과

고객의 현재 시스템 변동 없이 모든 것이 준비된 씨디네트워크스의 DDoS 방어 인프라와 보안 전문 인력 모두를 이용할 수 있습니다. 마치 보험처럼 계약만으로 즉시 고객 시스템의 DDoS 방어 용량을 수 배 증가시킬 수 있습니다.

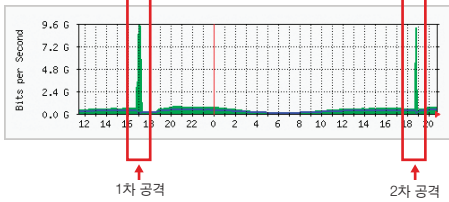


- 기존 고객 시스템 유지하면서 방어 용량 증가 (자체 방어 시스템 구축이나 시스템 이전 불필요)
- 대규모 방어 인프라에 의한 극한적 공격에도 고객 비즈니스 연속성 보장
- 다수 보안관제인력에 의한 모든 유형의 공격 대상 신속한 방어 및 서비스 재개 보장

케이스 스터디

기존 DDoS 방어의 한계를 넘어선 국내 유일의 DDoS 방어 시스템인 씨디네트워크스의 Secured Hosting은 국내 유수의 포털 사이트 및 쇼핑몰을 대상으로 안전하게 서비스하고 있습니다.

■ A사 케이스 (대역폭 고갈형 공격 방어)



2009년 4월 5일, 4월 6일 2차례 연이은 공격 발생

- 공격 (Zombie) 내역 : 555개
 - KT : 200여개, SKBroadband : 100여개, Dacom : 50여개, 기타 : 93개
 - C&C : gks.zef.cn 외 2개 Domain
- 공격 트래픽 : Max 15Gbps

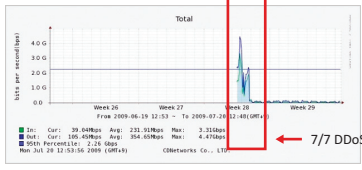
■ 1차 공격 조치 내역

- 16 : 35분 보안관제센터 고객사 공격 감지
- 16 : 36분 GSLB에서 트래픽 우회 작업 수행
- 16 : 38분 트래픽 우회 완료
- 16 : 43분 Secured Zone으로 공격 시작 및 차단
- 17 : 17분 공격 종료

■ 2차 공격 조치 내역

- 18 : 51 보안관제센터 공격 감지
- 18 : 51 1차 공격으로 기 우회된 Secured Zone으로 공격 시작 및 차단
- 19 : 10 공격 종료

■ B사 케이스 (자원 고갈형 공격 방어)



2009년 7월 7일, DDoS 대란 발생

- 공격 유형 : HTTP Get Flooding 공격
- 공격 트래픽 : Max 4Gbps

■ 7월 8일 09 : 10 고객 서비스 불가, 트래픽 우회 요청 접수

- 09 : 40 GSLB에서 트래픽 우회 작업 수행
- 09 : 45 Secured Zone으로 공격 시작 및 차단
- 10 : 40 Get Flooding 공격으로 서버 자원 부족 시큐어드 서버 2대 추가, 총 5대
- 14 : 43 지속적인 공격 IP 추출 차단 집중, 방화벽과 iptable 활용 차단, 시큐어드 서버 2대 추가, 총 7대

- 18 : 00 공격 종료 트래픽 하강
- 19 : 55 공격 재시작 트래픽 상승
- 23 : 50 시큐어드 서버 2대 추가, 총 9대

■ 7월 9일 18:00 추가 공격 시작

■ 7월 10일 18:00 공격 종료

Accelerating Your World

씨디네트웍스는 세계적인 CDN(Content Delivery Network, 콘텐츠 전송 네트워크) 서비스 전문기업으로 세계 50여 개 도시, 80여 개 POP의 네트워크 및 서버 인프라를 기반으로 미디어 스트리밍, 대용량 파일 전송, 웹 가속 서비스 분야에서 독보적인 기술력을 선보이며 전세계 CDN 비즈니스 시장을 이끌어 가고 있습니다. 첨단 테크놀로지를 이용한 씨디네트웍스 서비스의 모든 것은 씨디네트웍스 상품체험사이트에서 경험하실 수 있습니다.

서울특별시 강남구 역삼동 828-7호 한동빌딩 2층(135-935) Tel. 02-3441-0400 E-mail. inquiry@cdnetworks.co.kr www.cdnetworks.com | www.nextcdn.com

Copyright©CDNetworks. All rights reserved.