AhnLab

Case Study

금융권 디도스 공격 실전 대응 가이드

Contents

개요

계속되는 디도스 공격, 실질적인 해결책은?

2021년 국내 인터넷 환경을 위협할 주요 경계 대상 중 하나는 바로 '분산 서비스 거부 공격(Distributed Denial of Service: DDoS)'이다. 코로나19로 인한 비대면(언택트) 흐름에 따라 트래픽 사용량이 급증하고 있으며, 분산 서비스 거부 공격(이하 디도스) 공격 역시 증가하는 추세를 보이고 있다.

최근의 디도스 공격은 국가 지원을 받는 글로벌 해킹 그룹 주도 하에 비트코인, 랜섬웨어와 결합하여 직접적인 금전 이익을 노린다. 디도스 방어에 관한 딜레마는 공격자 IP를 알아내더라도, 공격하는 사람은 찾기 어렵다는데 있다. 여기에 비트코인 기술의 익명성이 더해져, 공격자들은 더 노골적으로 기업을 공략하고 금전을 요구하고 있다.

국내 네트워크 환경은 디도스 공격 대응 체계가 잘 갖춰져 있다. 네트워크 구간에 디도스 대응 솔루션을 설치하고, 정기적인 모의 훈련을 진행해 방어 준비를 철저히 하고 있다. 그럼에도 불구하고 매년 디도스 공격으로 인한 피해 사례가 언론에 노출되고 있으며, 많은 기업의 보안 담당자들이 디도스 공격에 대한 실전 대응 방안을 고민하고 있다.

결국 핵심은 실전 대응이다. 아무리 좋은 솔루션을 설치했더라도 제대로 된 사용법을 모르면 그야말로 '무용지물'이라 할 수 있다.

금융권 디도스 공격 현황

금융업계는 산업의 특성상 공격자들의 주요한 표적이 되곤 한다. 2020년 금융권을 향한

디도스란?

다수의 PC를 봇넷으로 감염시킨 후 공격 대상 서버에 일제히 공격을 가해 과부하로 인한 피해를 입히는 공격 방식.

디도스 공격은 은행, 증권, 금융 공기업, 핀테크 업체를 대상으로 많이 발생했다. 금융권 조직이 디도스 공격을 받아 다음과 같은 일이 발생한다고 가정해보자.

"특정 시점에 주식 거래가 정상적으로 되지 않는다면?"

"약속된 시점에 자금 이체가 되지 않는다면?"

만약 위와 같은 일이 벌어진다면, 금융 회사에 유무형의 금전적인 손실을 유발할 것이다. 이러한 유무형의 손실을 무기 삼아, 금전적 요구를 하는 '국가 지원 글로벌 해킹 그룹'의 공격이 많아졌다. 2020년 감행된 디도스 공격 중 많은 사례가 글로벌 해킹 조직의 '랜섬 디도스(Ransom DDoS)'였다. 랜섬 디도스는 디도스 공격 기법 중 하나로, 실질적인 공격 구성은 기존과 크게 다르지 않다.

우선 디도스 공격의 모든 종류에 대해 살펴보자.

디도스 공격 정리

디도스 공격을 공격 기법에 따라 나눠 정리하면 다음과 같다.

공격 기법	설명
DoS (Denial of Service)	• 가장 기본적인 공격 • 단일 클라이언트 → 특정 서버에 수행하는 공격 (1:1)
DDoS (Distributed Denial of Service)	• 다수의 PC를 봇넷(Botnet)으로 감염, 특정 시점에 공격 • 다수 클라이언트 → 특정 서버에 수행하는 공격 (N:1)
DRDoS (Distributed Reflection DoS)	• 반사체를 활용한 UDP 디도스 공격 • Tbps급 초대용량 공격 유발
APDoS (Advanced Persistent DoS)	• APT 공격을 위한 수단으로서의 디도스 공격 • 디도스로 관리자의 시선을 유도 후, APT 등 공격 수행 • 멀티 벡터 디도스 공격을 지칭하기도 함
Ransom DDoS (DDoS Extortion)	• 금전적 보상을 위한 협박성 공격 • 협박을 위한 실력 과시용 디도스 공격을 동반
DDoS as a Service	• 일종의 디도스 공격 대행 서비스 • 공격 규모와 기법에 따라 요금이 다름

[표 1] 디도스 공격 기법

디도스 공격에도 장르가 있다?

디도스 공격은 공격 기법과 트래픽 양에 따라 다양한 방법이 존재한다. 흔히 알려진 디도스도 공격 기법 중 하나이다.

또한, 디도스 공격은 트래픽의 양을 기준으로 다음과 같이 정리할 수 있다.

대용량 트래픽

TCP Flooding: TCP의 구성 요소를 섞어서 수행하는 공격이다. SYN과 ACK가 주를 이루며, XMAS, NULL과 같은 TCP 공격도 가능하다.

UDP Flooding: UDP의 특성을 활용한 공격으로 DRDoS와 결합 가능하다. '비 연결성/비 신뢰성'이라는 UDP 프로토콜의 특성으로 인해, 공격 수행 난이도가 낮다. Memcached, SNMP, CHARGEN, DNS, NTP 등 프로토콜의 이름이 강조되는 경우 UDP Flooding 공격으로 분류할 수 있다.

SSL Flooding: SSL/TLS를 활용한 대용량 디도스 공격으로, SSL/TLS의 특성상 트래픽 생성과 대량 생성이 어렵다.

HTTP Flooding: HTTP 프로토콜을 활용한 디도스 공격으로 GET, POST 등 HTTP의 요청 메소드(Method)별 공격이 존재한다.

Fragmentation Flooding: IP 패킷의 단편화를 통해 수행하는 디도스 공격이다.

저용량 트래픽

저용량 정밀 타격: 디도스 대응 솔루션의 제 1 정책 '임계치 기반 대응'을 우회하기 위한 방법으로, 세션을 지속적으로 맺고 끊지 않거나 서버의 자원을 점유해 고갈시키는 방식이다. 예로는 Exhaustion Attack이 있으며, 인증 기반의 대응이 필요하다.

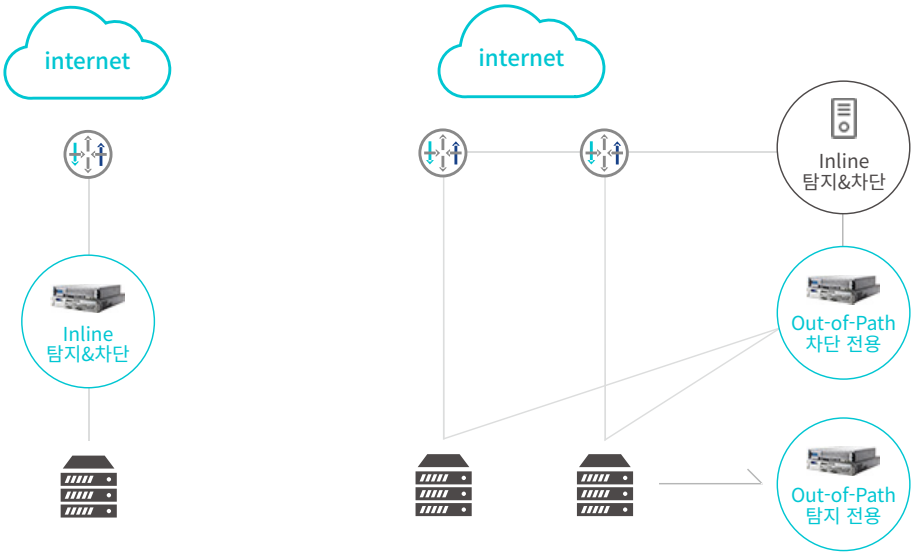
비정상 프로토콜: 프로토콜의 규칙을 위반한 공격으로 취약점의 형태로 발견해 대응되는 경우가 많다. 웹방화벽(WAF), 침입방지시스템(IPS), 디도스 솔루션을 통한 통합 대응이 필요하다. 공격 예시로는 Ping of Death, TearDrop, Slowloris, Slowread, LAND, Rudy, Smurf 등이 있다.

금융권 디도스 대응 솔루션 설치

디도스 대응 솔루션은 2가지 설치 방법을 제공한다. 'Inline'과 'Out-of-Path' 방식이다. 금융권의 99% 이상이 Inline 방식으로 디도스 솔루션을 설치한다. 빠른 디도스 공격 대응이 중요하기 때문이다.

디도스 솔루션 설치는 어떻게 하나?

네트워크 구간 내 설치하는 Inline과 외부에 설치하는 Out-of-Path 방식이 있다. Inline은 민첩성, Out-of-Path는 안정성이 강점이며 금융권은 Inline 방식을 주로 사용한다.



[그림 1] Inline vs Out-of-Path 구성 방식

두 설치 방식의 주요 특징을 비교하면 다음과 같다.

분류	Inline	Out-of-Path
필요 장비 수	1대 (탐지 & 대응)	2대 (Detector: 탐지, Guard: 차단)
설치 난이도	낮음	높음
DDoS 대응 속도	매우 빠름	빠름
장애 발생 확률	낮음	매우 낮음
고객 분류	공공기관, 금융, 학교	인터넷 서비스 제공자(ISP), 포털, 데이터센터(IDC)

[표 2] Inline vs Out-of-Path 비교

솔루션의 발전에 따라 디도스 공격의 탐지 및 대응 관점에서 두 설치 방식에 큰 차이는 없다. 하지만 구성의 근본적인 특성으로 인해, 설치 방법이 업계별로 확연하게 구분된다.

금융권 디도스 대응 방법

금융권에서는 다음과 같이 디도스 대응 전략을 수립해 실천하고 있다.

Step 1: 임계치(Threshold) 기반 규칙 방어

모든 디도스 대응 솔루션은 임계치 기반 규칙을 포함하고 있다. 임계치 기반 규칙은 패킷

디도스 대응법 1: 임계치 기반 규칙

기준치 이상의 트래픽이 발생할 경우 디도스 공격으로 탐지해 대응하는 기법. 정상 사용자 차단의 위험이 있고 저용량 공격 대응 측면에서 한계가 있다.

의 구성 요소를 일일이 셈하여, 기준치 이상의 트래픽이 발생할 경우 디도스 공격으로 탐지해 대응하는 기법이다.

임계치 기반 규칙은 크게 '도스(DoS)'와 '디도스(DDoS)' 규칙으로 구분한다. 도스의 경우 단일 출발지 IP를 기준으로 패킷의 양을 측정하며, 단일 IP에서 트래픽이 많이 들어오는 관계로 즉각 차단하더라도 문제가 적어 차단·격리 방법으로 주로 대응한다. 반면 디도스는 다수의 출발지 IP 기준, 보호 대상에 인입되는 트래픽의 양을 측정한다. 단 디도스의 경우 특정 이벤트에 따라 트래픽이 많아지는 경우가 있어 단순히 차단을 할 경우 수많은 정상 사용자를 차단할 위험이 있다. 그러므로 인증을 통한 추가 검증 또는 QoS(Quality of Service)를 수행한다.

분류	도스(Dos) 임계치 규칙	디도스(DDoS) 임계치 규칙
측정 기준	단일 출발지 IP 기준, 보호 대상에 인입되는 패킷의 양	다수 출발지 IP 기준, 보호 대상에 인입되는 패킷의 양
대응 방법	차단, 격리	인증, QoS, 격리
규칙 예시	DoS_TCP_SYN: 500pkts/1초	DDoS_UDP: 10000pkts/2초
규칙 설명	단일 출발지 IP 기준 초당 500개의 TCP SYN이 보호대상으로 인입되는 경우 도스 공격으로 탐지 및 대응	다수 출발지 IP기준 2초당 10,000개의 UDP가 보호 대상으로 인입되는 경우 디도스 공격으로 탐지 및 대응
단위	PPS(Packet Per Second) BPS(Bit Per Second) CPS(Connection Per Second)	

[표 3] 도스 & 디도스 임계치 규칙

안랩의 디도스 공격 대응 솔루션 'AhnLab DPX'의 경우 네 가지 종류, 약 60여개의 임계치 기반 규칙과 사용자 정의 임계치 기반 규칙을 제공하고 있다.

※**주의사항:** 임계치 규칙의 경우 일상적인 대용량 공격 대응에 적합하지만, 저용량 정밀 타격 또는 비정상 프로토콜 공격에는 대응이 어렵다.

Step 2: 인증 기반 대응

모든 디도스 솔루션이 임계치 기반 대응 역량을 제공하며, 고객도 해당 기능을 무리 없이 사용하는 편이다. 하지만, 실질적으로 발생하는 디도스 공격의 피해 사례는 임계치 기반 규칙을 우회하는 공격이다. 실제 2020년 국내 금융권에서 해당 공격으로 인한 서비스 장애 현상이 많이 발생하였으며, 이러한 공격은 인증 기능으로 대응해야 한다.

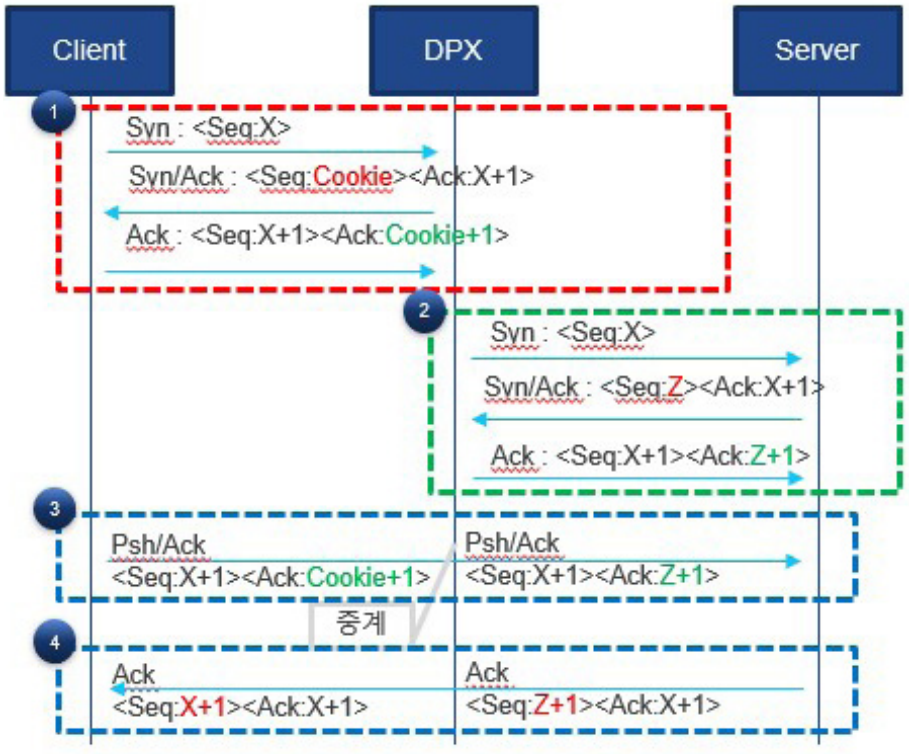
디도스 대응법 2:
인증 기법

인증을 통해 클라이언트가 봇인지 여부를 탐지해 대응하는 기법. 디도스 공격의 99%가 봇을 통해 수행되어 방어에 효과적이다.

인증 기반 대응은 주로 봇(Bot) 기반의 자동화된 공격을 방어한다. 즉 저용량 공격이더라도 봇을 활용할 경우 해당 인증 기법으로 대응할 수 있다. 대부분의 디도스 공격은 사람이 직접 수행할 수 없다. 99% 이상이 자동화 소프트웨어(봇)을 활용하며, 이러한 공격은 인증을 통해 대응이 가능하다.

여기서 '인증'은 TCP와 HTTP 프로토콜의 특성을 활용한 기법이다. AhnLab DPX의 경우 TCP와 HTTP 각각 세 가지, 총 여섯 가지 기법을 제공한다. 이러한 기법은 한국인터넷진흥원(KISA)이 발간한 'DDoS 공격 대응 가이드 – 2012. 10'에도 명시되어 있는 보편적인 디도스 대응 기법으로, 타사 디도스 솔루션 역시 부분적으로 인증 기능을 제공한다.

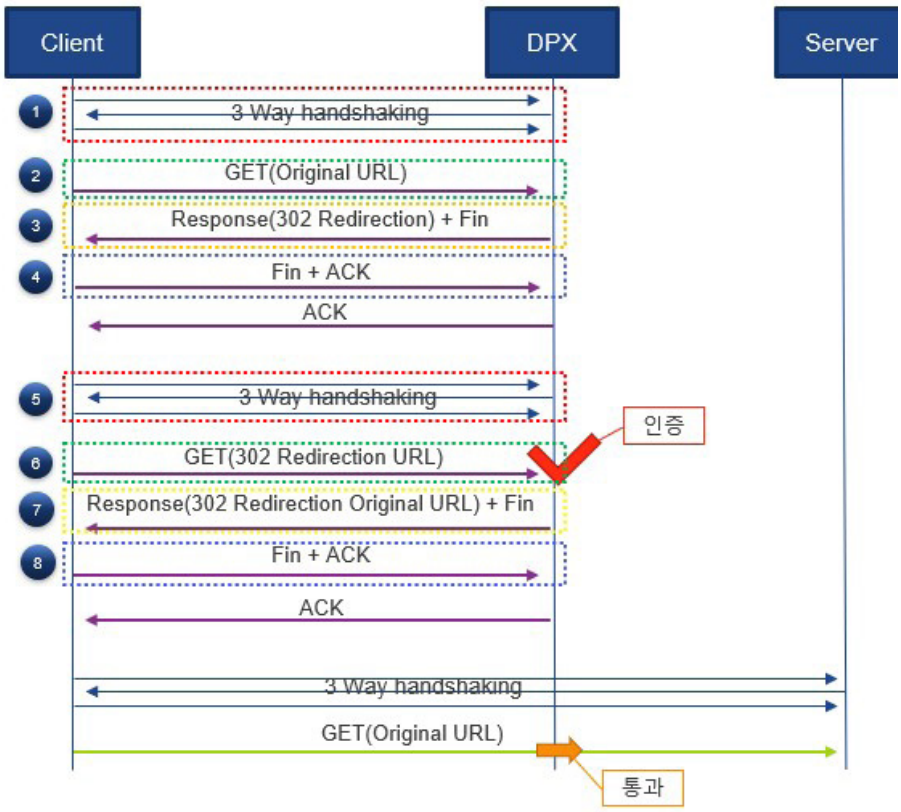
TCP 인증의 경우 최초 클라이언트(Client)의 SYN 패킷에 일종의 쿠키(COOKIE)를 추가한 SYN/ACK 응답을 생성하여, 쿠키가 포함된 ACK가 전송되는지 확인하는 방법이며, RST을 활용한 방법도 있다. HTTP 인증의 경우 HTTP 302 응답코드를 활용해, 정상적인 리다이렉트(REDIRECT)가 진행되는지 확인하는 방법이다.



[그림 2] TCP 인증 기법

인증 기법의 효과

인증 기법을 활용하면 저용량 및 고용량 트래픽 공격과 비밀번호 무작위 대입 등 다양한 디도스 공격 대응이 가능하다.



[그림 3] HTTPS 인증 기법

위와 같은 방식으로 클라이언트가 정상 사용자인지, 디도스 공격을 수행하는 봇인지 탐지해 대응한다. 이러한 인증 기능을 수행할 경우 봇 기반의 디도스 공격에 효과적으로 대응할 수 있다.

또한, HTTP 디도스 공격의 일종인 Bruteforce(비밀번호 무작위 대입) 공격 역시 인증 기능을 통해 방어할 수 있다. 아래는 실제 비밀번호가 password인 경우 인증 기능 활성화 여부에 따른 서버의 응답 길이를 보여준다. 인증 기능을 활성화한 경우, 봇을 인지하여 일정한 길이(203)의 응답을 제공함을 알 수 있다.

분류	설명
조건	비밀번호 → password
인증 Off	password로 대입할 경우에 응답이 다름을 확인하여 실제 비밀번호 유추 가능
인증 On	password로 대입할 경우에 302 Status와 동일한 길이의 응답이 제공되어 실제 비밀번호 유추 불가능

[표 4] 인증 기능을 통한 Bruteforce 공격 방어 시나리오

디도스 대응법 3:
하이브리드 디도스 대응

초대용량 디도스 공격은 인증 기법으로 대응이 어렵다. 다만, 공격 용량이 작아지는 추세이므로 비상 대책으로 하이브리드 디도스 대응을 고려 가능하다.

Request ▲	Payload	Status	Error	Timeout	Length
1	passqwer	200	☐	☐	4584
2	passqwww	200	☐	☐	4584
3	passwedd	200	☐	☐	4584
4	passwfgg	200	☐	☐	4584
5	password	200	☐	☐	4627
6	passcwer	200	☐	☐	4584
7	passwora	200	☐	☐	4584
8	passworb	200	☐	☐	4584
9	passworc	200	☐	☐	4584
10	passwork	200	☐	☐	4584

Request ▲	Payload	Status	Error	Timeout	Length
1	passqwer	302	☐	☐	203
2	passqwww	302	☐	☐	203
3	passwedd	302	☐	☐	203
4	passwfgg	302	☐	☐	203
5	password	302	☐	☐	203
6	passcwer	302	☐	☐	203
7	passwora	302	☐	☐	203
8	passworb	302	☐	☐	203
9	passworc	302	☐	☐	203
10	passwork	302	☐	☐	203

필터	프로토콜	출발지 IP	목적지 IP	목적지 포트	차단 (bytes)
HTTP 접속 인증	TCP	172.20.32.102	192.168.101.65	80	10,021

[그림 4] 인증 기능을 통한 Bruteforce 공격 방어

이처럼 TCP/HTTP 인증 기능을 통해 봇 기반 '저용량 정밀 타격'과 '비정상 프로토콜' 공격을 방어할 수 있으며 기타 봇 기반의 공격을 방어한다. AhnLab DPX의 경우 총 여섯 가지 기법을 제공하면서도 실망에서 사용 가능한 성능을 제공하는 것이 최대 강점이다.

※**주의사항:** 만약 100Gbps ~ 1Tbps 이상의 초대용량 공격이 들어오면, 임계치 기반 규칙 또는 인증 기능으로 방어할 수 없다.

Step 3: 하이브리드 디도스 공격 대응

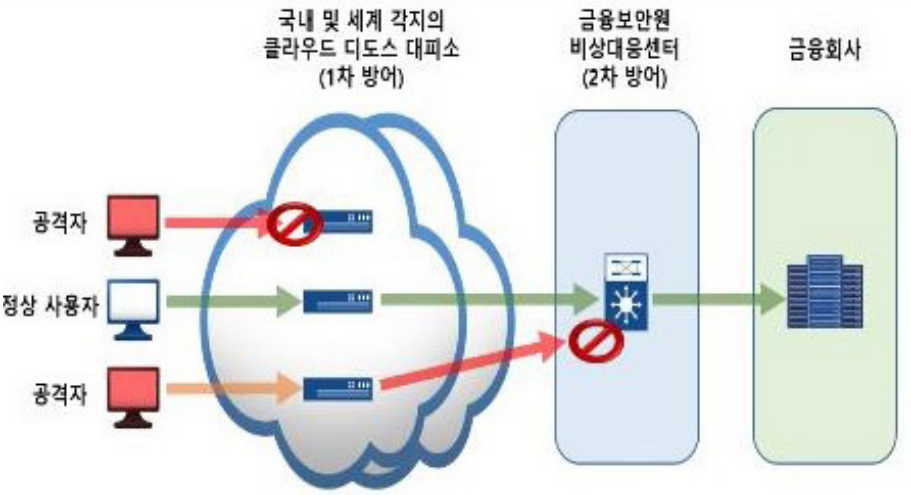
2018년, 소스코드 저장소로 유명한 깃허브(Github)를 대상으로 1Tbps 이상의 디도스 공격이 발생했다. 일반적인 기업의 경우, 사용 중인 회선의 대역폭(1G, 10G) 이상의 디도스 공격이 발생할 경우 대응할 수 있는 방법이 마땅치 않다.

하지만, 반드시 유지되어야 하는 서비스에 대해서는 초대용량 디도스 공격을 방어할 수 있는 방법이 필요하다. 우리나라 금융권의 경우 금융보안원이 제공하는 서비스형 보안

디도스 완벽 방어 가능한가?

디도스 공격 100% 방어는 불가능에 가깝다. 성공적인 '완화'에 초점을 두면서 디도스 대응 솔루션의 기능을 적절히 사용하고 실전 대응 역량을 기르는 것이 중요하다.

(SECurity-as-a-Service) 형태의 디도스 공격 대응 서비스 '스크러빙센터'의 보호를 받을 수 있다. 해당 대응 체계는 ▲1차 방어 – 스크러빙센터 ▲2차 방어 – 금융보안원 비상대응센터 ▲3차 방어 – 금융회사 자체 디도스 대응으로 구성되어 있다.



[그림 5] 금융권 대용량 디도스 공격 대응체계 (출처: 금융보안원 보도자료)

국내 보안회사는 초대용량 디도스 공격 방어를 위한 스크러빙센터를 제공하고 있지 않다. 2018년 이후 디도스 공격의 최대 규모가 점차 감소하고 있으며, 실질적으로 국내 일반 기업이 초대용량 디도스 공격에 노출될 가능성이 굉장히 낮기 때문이다. 실제 스크러빙센터를 이용할 경우 높은 수준의 비용이 청구되는 관계로, 실제 사용 고객은 극히 적은 편이다. 즉, 스크러빙센터는 혹시 모를 초대용량 디도스 공격 방어를 위한 비상 대응 방안으로 고려 가능하다.

앞서 다룬 내용을 종합하면, 국내 금융회사들은 금융보안원의 보호를 받고 있으며, 자체적으로 견고한 디도스 대응 체계를 구축하고 있다. 자체적인 디도스 대응 체계의 경우 ▲임계치 기반 규칙 ▲TCP/HTTP 인증 기법을 활용하고 있다. 이에 더해, 시그니처 기반 대응, QoS, 접근제어목록(Access Control List: ACL) 등을 활용하여 디도스 공격을 방어하고 있다.

모든 디도스 공격을 100% 방어하는 것은 불가능에 가깝다. 영어로도 디도스 공격 대응을 표현할 때 방어가 아닌 완화(Mitigation)라는 단어를 주로 사용하며, 성공적인 완화를 위해서는 디도스 대응 솔루션의 모든 기능을 적절히 사용하는 것이 필요하다.

슬기로운 AhnLab DPX 사용법

AhnLab DPX는 앞서 설명한 기능들을 모두 제공하며, 국내 네트워크 환경에서 견고한 디

Why AhnLab DPX?

프로스트앤설리번 국내 디도스 대응 솔루션 시장점유율 1위에 빛나는 AhnLab DPX. 유연한 설치, 10단계 필터, 실시간 패킷 탐지 등 다양한 디도스 대응 역량을 제공한다.

도스 대응 체계 조성에 앞장서고 있다. 또한, 타사 대비 우수한 성능을 제공해 시장조사기관 프로스트앤설리번(Frost & Sullivan)이 발표한 국내 디도스 대응 솔루션 시장점유율 1위를 기록하며 가장 많은 고객들의 선택을 받고 있다.

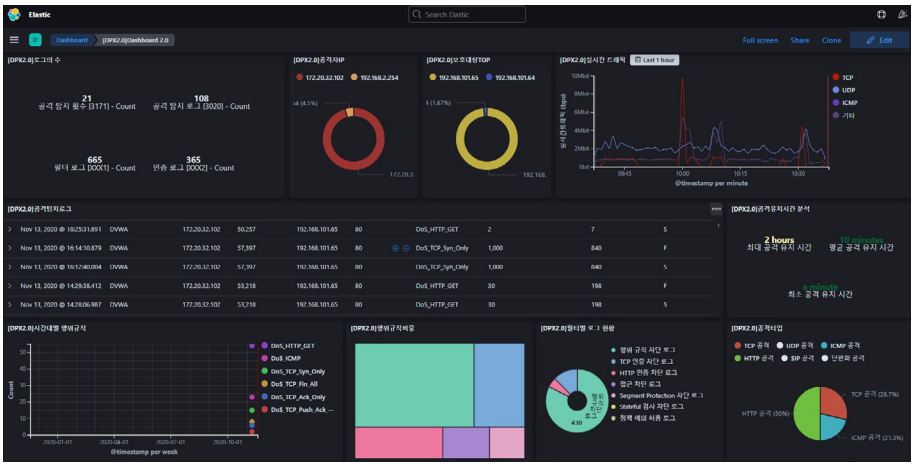
또한, AhnLab DPX는 다음과 같은 기능들을 추가적으로 제공한다. 디도스 공격에 슬기롭게 방어할 수 있도록 AhnLab DPX가 제공하는 주요 기능 세 가지를 알아보자.

슬기로운 방어 1: Zone 기능(Multi-Tenancy)

여러 개의 보호 대상을 각각 'Zone'이라는 개념으로 설정하여, 각 대상에 대한 관리를 완전히 분리해 수행할 수 있다. AhnLab DPX는 최대 328개의 Zone을 제공하며, 정책 설정, 로그 모니터링을 개별 Zone 기준으로 수행 가능하다.

슬기로운 방어 2: 다양한 로그 연동

외부 SIEM(Security Information & Event Management) 및 빅데이터 플랫폼과 연동해 로그 가시성을 확보하고 빅데이터 분석을 수행할 수 있다. 제품에서 발생하는 로그 모두를 외부로 전송 가능하며, 일종의 고성능 트래픽 센서로 디도스 대응 솔루션을 사용할 수 있다.



[그림 6] Elasticsearch 연동, Kibana 대시보드

또한 실시간 트래픽 현황을 확인할 수 있고, 공격의 공격 시간 파악 및 이상 공격을 파악해 분석 가능하다.

슬기로운 방어 3: API 연동

이제 SIEM을 넘어 SOAR(Security Orchestration Automation & Response)의 시대가 오고 있다. AhnLab DPX는 안랩의 보안 운영 효율화 플랫폼 'AhnLab Sefinity AIR'를 비롯, 다양한 SOAR와 로그 연동 및 Rest API를 통해 대응 정책 자동화를 구현할 수 있다. 특

"AhnLab DPX의 최대 강점은 바로 '연결성'이다. 제품의 탁월한 기능에 컨설팅, 관제 서비스, 모의 훈련 서비스 및 안랩이 보유한 다른 솔루션들의 역량이 유기적으로 더해져 고객에게 최상의 디도스 대응 프로세스를 제공한다."

히 SIEM과 SOAR 등의 시스템을 통한 관제 업무에 있어, API 연동을 통한 위협 대응 자동화는 필수로 자리잡았다. AhnLab DPX는 AhnLab TMS와의 연동을 통해 통합 정책/로그 관리 및 Rest API를 지원한다.

AhnLab DPX에 대한 보다 자세한 사항은 안랩 공식 홈페이지에서 확인 가능하다.

▶AhnLab DPX 제품 소개 페이지 바로가기

▶AhnLab DPX 소개 영상 바로가기