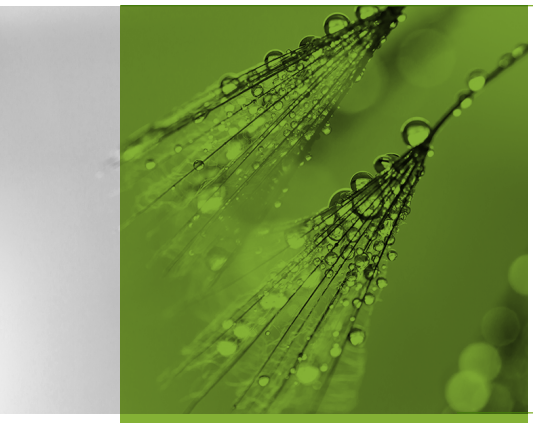

corero

주니퍼 네트웍스와 CORERO: 대규모 DDOS 방어를 위한 현대적인 접근

경제적인 비용으로 대규모(volumetric) DDoS 공격 실시간 탐지 및 방어

과제

오늘날의 위협에서 중요한 부분을 차지하는 DDoS 공격은 규모, 빈도 및 정교함 면에서 진화를 거듭하고 있습니다. 기존의 아웃오브밴드(out-of-band) 스크러빙센터와 수동 개입 방식으로는 증가하는 위협 문제를 해결할 수 없습니다.

솔루션

주니퍼와 Corero가 개발한 혁신적인 최신 DDoS 공격 방어 솔루션은 네트워크 에지 전반에서 상시 패킷 레벨 모니터링, 자동화된 머신 분석, 인프라 기반 실행을 활용하여 실시간으로 회선 속도 수준의 탐지와 방어를 제공합니다.

이점

- *네트워크 에지에서 악성 트래픽을 차단함으로써 DDos 방어 비용 절감*
- *자동화된 대응으로 수 초 내에 DDoS 공격 차단*
- *상시 패킷 레벨 모니터링으로 가시성을 향상시키고 공격 전후/진행 중에 즉시 대응할 수 있는 인텔리전스(Actionable Intelligence) 제공*
- *초당 수십 테라바이트로 방어 용량 확장*

인터넷 시대가 시작된 이후로 디도스(DDoS) 공격은 일종의 항의, 피해 야기, 경쟁사 방해, 보복 등에 사용되어 왔습니다. DDoS는 압도적인 트래픽 양으로 웹사이트, 네트워크 및 클라우드 트래픽을 증가시킴으로써 가동 중단과 서비스 다운타임을 야기하고 일상의 모든 면을 서비스 프로바이더와 엔터프라이즈 네트워크에 의존하는 일반 사용자의 합법적인 액세스를 가로막습니다. 2017년 비즈니스의 디도스DDoS 공격 대응을 위한 평균 비용은 250만 달러 이상으로 증가한 것으로 추정됩니다.[1].

과제

오늘날에는 코딩 경험이 전무하다 할지라도 누구든지 100달러 미만의 비용으로 손쉽게 DDoS 공격을 실행할 수 있습니다.

공격 대행 서비스는 기술적 역량이나 비용 측면 모두에서 이러한 공격을 수행하는 범법자의 진입 장벽을 낮추는 결과를 초래했습니다. IoT(Internet of Things)의 증가로 인해 기본적으로 내장된 보안이 없는 대규모의 커넥티드 디바이스들은 해커들이 선호하는 공격 대상이 되고 있습니다. 2016년, Mirai IoT 봇넷은 전 세계적으로 약 10만 대의 커넥티드 디바이스를 손상시켰습니다. 감염된 디바이스는 DNS(Domain Name System) 서비스 프로바이더 Dyn에 대해 최대 용량 초당 1.2테라바이트(Tbps) DDoS 공격을 감행하여 4시간 이상의 서비스 중단 및 다운타임을 초래했습니다. Mirai는 시작에 불과했습니다. 그 후 JenX, Hajime, Satori, Reaper 등과 같은 변종이 발생하면서 공격이 점점 더 정교해지고 있으며, 그만큼 방어하기도 어려워지고 있습니다.

DDoS 공격 대행 서비스가 증가하고 보안 솔루션 없는 IoT 디바이스가 수십 억대로 증가하면서 DDoS 공격도 높은 증가세를 보이고 있습니다. 최근 Corero의 **DDoS 동향 및 분석** 보고서에 따르면 기업들은 2017년 3분기 동안 매월 평균 237건의 DDoS 공격 시도를 확인한 것으로 나타났으며, 이는 전년 분기 대비 35% 증가한 수치로 매일 8건의 공격 시도를 받았다는 것을 의미합니다. 5G 모바일 네트워크로의 전환으로, 사용 가능한 대역폭이 증가하고 감염된 커넥티드 디바이스가 공격 트래픽을 생성할 수 있는 더욱 강력한 파이프라인이 조성되면서 문제는 더욱 복잡해졌습니다.

[1] https://www.zdnet.com/article/the-average-ddos-attack-cost-for-businesses-rises-to-over-2-5m/

DDoS 공격의 빈도, 크기, 정교함이 증가함에 따라 아웃오브밴드 스크러빙센터(scrubbing center), 수동 개입 등과 같은 기존의 방어망은 더 이상 통하지 않을뿐더러 막대한 비용도 유발합니다. 대규모 공격의 경우 의심스러운 트래픽을 스크러빙센터로 리디렉션하려면 지연 시간이 증가할 뿐 아니라 방어 비용이 데이터 트래픽의 양과 직접적인 연관이 있으므로 재정적으로 엄청난 부담을 초래합니다. 이러한 기존 접근 방식에는 수동 분석 및 인적 개입도 필요하므로 문제 해결 프로세스의 지연 시간이 더욱 늘어나고 대응을 위한 비용 소모도 높아집니다. 기존 방법을 사용하면 탐지 및 대응 사이에 최대 30분이 경과할 수 있으며, 이러한 대응 속도는 DDoS 공격으로 몇 분 내로 웹 사이트가 다운될 수 있는 시대에는 너무 느립니다.

항시 접속이 필요한 시대에 다운타임은 모든 기업에게 큰 문제가 될 수 있습니다. 서비스 프로바이더와 엔터프라이즈는 기존 DDoS 방어 전략을 재검토하고 더 낮은 비용으로 더욱 빠르고 효과적인 보호를 제공하는 새로운 기술을 고려해야 합니다. IP 네트워크는 대규모 공격에 대한 1차 방어선으로서 솔루션의 핵심적인 부분이 되어야 합니다. 텔레메트리, 머신러닝 및 네트워크 프로그래밍 기능은 더욱 지능적이고 자동화된 어댑티브 탐지 및 방어 프로세스를 구축할 수 있도록 지원합니다.

주니퍼 네트웍스와 Corero DDoS 보호 솔루션

주니퍼 네트웍스는 Corero Network Security와 협력하여 빠른 식별, 정교한 의사 결정, 네트워크 내 전략적 지점에서의 자동화된 대응, 지속적인 모니터링을 통해 네트워크의 자가 복구를 실행하는 DDoS 방어 조인트 솔루션을 개발했습니다(그림 1).

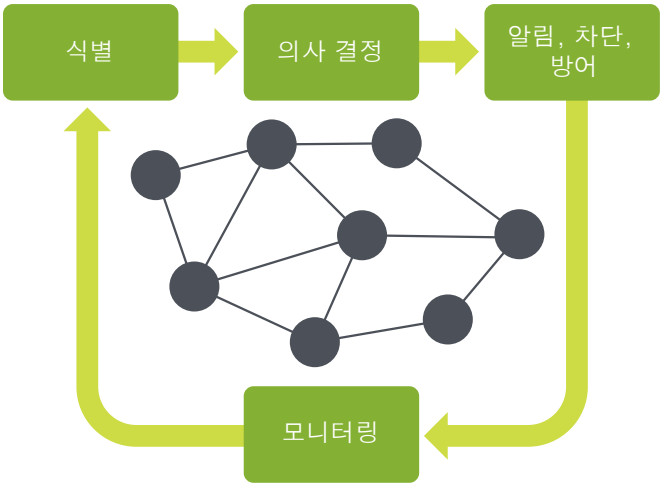

그림 1: 자가 복구 네트워크

효과적인 DDoS 방어를 위한 가장 좋은 방법은 가능한 한 소스에 가까운 곳(일반적으로 네트워크 에지)에서 공격을 차단하는 것입니다. 따라서 일반적인 DDoS 차단 지점 세 곳은 서비스 프로바이더 피어링 포인트, 데이터센터 에지, 가입자 에지입니다.

주니퍼 네트웍스와 Corero Network Security의 DDoS 조인트 솔루션은 매우 효과적이고 자동화되었으며 시중의 다른 DDoS 솔루션 대비 더 저렴한 비용으로 멀티테라바이트 용량으로 확장할 수 있습니다. 네트워크 에지에서 작동하며, 다음과 같은 기술을 사용하여 DDoS 공격을 탐지하고 이에 대응합니다(그림 2 참조).

- 네트워크 에지에 구축되는 주니퍼 네트웍스® MX 시리즈 5G 유니버설 라우팅 플랫폼은 헤더 및 페이로드를 모두 포함하는 샘플링된 미러를 통해 수신 트래픽을 모니터링하고 공격에 따라 동적으로 확장하여 위협 규모에 대응할 수 있습니다.
- MX 시리즈 라우터는 샘플링된 미러를 Corero SmartWall TDD(Threat Defense Director)로 포워드합니다. TDD는 규칙 기반 분석 및 머신 분석을 사용하고 피드의 모든 패킷을 검사하여 모든 DDoS 공격 트래픽을 빠르고 정확하게 탐지합니다.
- 몇 초 내에 TDD가 모든 공격을 식별하고 유연한 방화벽 일치 필터를 자동으로 생성하여 MX 시리즈 라우터를 통해 공격에 대응합니다.
- TDD는 NETCONF(Network Configuration Protocol)를 통해 MX 시리즈 라우터를 자동으로 구성하여 악성 트래픽 소스에 가장 가까운 수신 지점에 DDoS 공격을 차단하는 필터를 적용하는 임시 구성을 설치합니다. 또한 차단만큼 중요한 작업의 하나로 정상 트래픽은 포워딩 성능 저하 없이 대상 목적지로 이동할 수 있도록 합니다.
- MX 시리즈 라우터에서 스트리밍 텔레메트리는 허용/차단된 트래픽 통계를 Corero SmartWall TDD로 전달합니다.
- SmartWall TDD SecureWatch Analytics는 공격 전후 및 도중 네트워크 트래픽을 포괄적으로 파악할 수 있는 기능을 제공합니다. 이 Splunk 기반 애플리케이션은 운영팀에 공격 요약사항과 대응 프로세스 효과에 대한 실행 가능한 인텔리전스를 제공합니다.

이 프로세스는 미러링된 샘플이 수신 지점이 더 이상 공격받고 있지 않음을 나타낼 때까지 공격의 수명 주기 동안 계속됩니다. 이 시점 SmartWall TDD는 MX 시리즈 라우터에서 필터를 제거하고 정상적인 운영을 재개합니다. 미러링된 샘플과 스트리밍 텔레메트리는 MX 시리즈 라우터에서 Corero의 TDD로 계속 이동하여 트래픽 흐름이 정상으로 돌아오도록 보장하는 한편 다음 공격을 모니터링합니다.

이 운영 모델은 완전히 자동화되어 비즈니스 운영을 완벽하게 보호하고 운영 팀에 필요한 가시성을 항상 제공합니다.

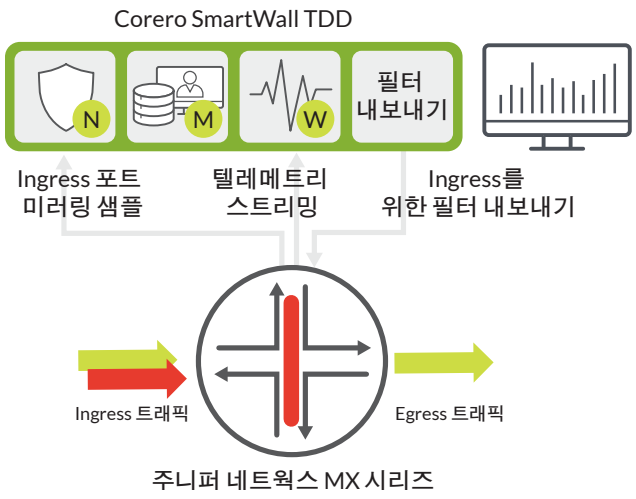

그림 2: 주니퍼 + Corero DDoS 방어 조인트 솔루션

기능 및 이점

주니퍼-Corero DDoS 방어 조인트 솔루션은 패킷 레벨에서 트래픽을 검사할 때의 이점과 인프라 기반 시행의 이점을 결합합니다. 이를 통해 전례 없는 수십 테라바이트 규모의 DDoS 공격을 실시간으로 자동 방어하는 동시에 비용을 대폭 절감합니다.

DDoS 방어 비용 절감

MX 시리즈 5G 유니버설 라우팅 플랫폼의 기존 필터링 기능을 활용함으로써 악성 트래픽은 분산된 네트워크 에지에서 제거됩니다. 공격 상황에서 모든 트래픽을 아웃오브밴드 중앙 스크러빙센터로 리디렉션하여 지연과 비용을 증가시키는 대신, 이 접근 방식은 서비스 프로바이더와 엔터프라이즈가 트래픽 볼륨에 따른 DDoS 방어 서비스 비용을 대폭 절감하는 동시에 값비싼 용량 업그레이드를 피할 수 있도록 해줍니다. 또한 조인트 방어의 95% 이상이 완전히 자동화되어 오퍼레이터 또는 분석가의 개입이 필요 없습니다. 이는 수동 개입에 크게 의존하는 기존 접근 방식 솔루션에 비해 TCO를 크게 낮춥니다.

신속한 대응 및 고객 만족도 향상

즉, 자동화란 DDoS 공격이 단 몇 초만에 식별되고 차단됨을 의미합니다. 수동 개입에 크게 의존했던 기존 접근 방식으로는 30분 이상이 소요되었던 작업으로, 이는 상당한 개선입니다. 속도는 핵심입니다. 감염되지 않은 트래픽이 계속 이동하도록 하고 공격 패킷만 선택적으로 차단함으로써 주니퍼-Corero 조인트 솔루션은 공격이 한창 진행 중인 순간에도 고객 비즈니스가 영향을 받지 않도록 보장합니다.

가시성, 리소스 효율성 및 방어 효과 향상

주니퍼-Corero 조인트 솔루션은 패킷 레벨에서 상시 모니터링을 지원합니다. 기존의 플로우 기반 탐지 방식에 비해 패킷 기반 검사는 효율성을 높이고, 운영자가 헤더 정보뿐만 아니라 페이로드 데이터도 보다 잘 파악할 수 있도록 합니다. 또한 IPFIX(IP Flow Information Export) 프로토콜과 비교해 보면, 샘플링된 미러링으로 라우터가 대량의 데이터를 집계 및 처리할 필요가 없으므로 라우터 리소스에 가해지는 부하가 매우 적습니다. 마지막으로, 조인트 솔루션은 립앤리플레이스(rip-and-replace)를 필요로 하지 않습니다. 네트워크 경계에서 IP 에지 라우터가 첫 번째 방어 라인인 계층형 DDoS 방어 모델의 기존 솔루션과 원활하게 작동하여 대규모 공격 트래픽을 오프로드하고 보다 정교한 애플리케이션 레이어 공격에 대응하기 위해 중앙 스크러빙 리소스를 사용합니다.

수십 테라바이트의 확장성

Corero SmartWall TDD는 네트워크에서 DDoS 트래픽을 백홀할 필요 없이 방어 용량을 회선 속도 수준인 최대 40Tbps까지 확장할 수 있습니다. MX 시리즈 5G 시리즈 유니버설 라우팅 플랫폼 및 최대 80Tbps의 패킷 포워딩 확장 기능이 결합된 이 조인트 솔루션은 오늘날 시장에서 제공되는 단일 DDoS 방어 시스템 중 최고의 확장성을 제공합니다.

솔루션 구성요소

Corero SmartWall TDD(Threat Defense Director)

Corero SmartWall TDD는 실시간 대규모 DDoS 방어를 위한 획기적인 솔루션으로 다음과 같은 기능을 제공합니다.

- 대규모 모니터링 및 방어 기능을 수십 테라비트까지 확장
- 정확한 볼륨메트릭 DDoS 탐지를 위한 패킷 레벨 검사
- 지능형 방어와 머신 분석을 통한 자동 필터링
- 실시간 대응을 통해 수 초만에 공격 대응
- DDoS 탐지 오작동을 제거하기 위한 폐쇄 루프 피드백
- 초, 분, 일, 주, 월 및 연도까지 확인할 수 있는 전체 로그
- 허용된 트래픽과 차단된 트래픽 모두에 대한 패킷 샘플 포렌식
- Splunk 기반의 강력한 분석, 보고, 알림 및 자동화
- 자동 대응 및 SecOps를 위한 개방형 통합 API
- BGP, NETCONF, REST(Representational State Transfer), JSON(JavaScript Object Notation) 및 클라우드를 통한 시그널링 완화

주니퍼 네트웍스 MX 시리즈 5G 유니버설 라우팅 플랫폼

MX 시리즈 플랫폼은 다음과 같은 기능을 제공하는 강력한 SDN 지원 라우터 포트폴리오를 제공합니다.

- 타의 추종을 불허하는 시스템 용량, 집적도, 보안 및 성능
- 처리량성능 저하없는 업계 최초의 인라인 데이터 플레인 보안
- 무제한 프로그래밍이 가능하여 지속적인 미래 혁신 지원
- 자동화를 통한 신속한 서비스 딜리버리
- 최대 40%의 TCO 절감 효과를 제공하는 멀티 서비스 네트워크 및 노드 슬라이싱 기능
- Junos® Continuity 및 Unified ISSU(unified in-service software upgrade)를 통한 다운타임 위험 감소
- 다양한 복원 기능 세트를 통한 탁월한 네트워크 및 서비스 가용성
- 심층 패킷 검사(DPI)를 통한 애플리케이션별 트래픽 처리
- JTI(Junos Telemetry Interface)를 통해 구성 요소 레벨 데이터를 모니터링하고 분석 툴로 스트리밍
- 최고의 공간 및 전력 효율성

요약—절감된 비용으로 실시간 DDoS 방어를 제공하는 현대적 접근 방식

멀티클라우드, IoT, 5G의 시대에 사이버 보안 위협은 끊임없이 진화하고 있습니다. 특히 DDoS 공격의 규모, 빈도와 정교함이 갈수록 진화하고 있습니다. 서비스 프로바이더와 엔터프라이즈 모두는 더 낮은 비용에 더 효율적이고 빠른 보호를 제공하는 솔루션을 통해 기존 방어 체계를 확대할 수 있는 방안을 모색해야 합니다.

IP 네트워크는 대규모 공격에 대한 첫 번째 방어선으로 현대 보안 솔루션의 핵심이 되어야 합니다. 텔레메트리, 머신러닝 및 네트워크 프로그래밍 기능은 더욱 지능적이고 자동화된 어댑티브 탐지 및 대응 프로세스를 구축할 수 있도록 지원합니다.

주니퍼-Corero DDoS 방어 조인트 솔루션은 패킷 레벨 트래픽 검사의 이점과 인프라 기반 실행의 이점을 결합합니다. 이를 통해 전례 없는 수십 테라비트 규모의 DDoS 공격을 실시간으로 자동 방어하는 동시에 비용을 크게 절감합니다.

다음 단계

주니퍼 네트웍스와 Corero가 악성 DDoS 공격으로부터 네트워크를 보호하는 데 어떻게 도움이 되는지 자세히 알아보려면 주니퍼 또는 Corero 판매 담당자에게 문의하세요.

Corero 소개

Corero Network Security는 실시간, 고성능 DDoS 방어 솔루션 부문의 리더입니다. 서비스 프로바이더, 호스팅 프로바이더 및 온라인 기업은 수상 경력에 빛나는 Corero의 기술을 활용하여 자사 환경에서 DDoS에 대한 위협을 제거하고 있습니다. Corero의 솔루션은 완벽한 네트워크 가시성, 분석 및 보고 기능과 함께 자동 공격 탐지 및 대응을 제공합니다. 업계를 선도하는 이 기술은 가장 복잡한 환경에서 DDoS 공격에 대한 비용 효율적이고 확장 가능한 보호를 제공하는 동시에 기존 출시 제품보다 더 비용 효율적이고 경제적인 모델을 가능케 합니다. 자세한 내용은 www.corero.com을 참조하십시오.

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 세상을 연결하는 제품, 솔루션, 서비스를 통해 네트워크를 간소화합니다. 주니퍼는 엔지니어링 혁신을 통해 클라우드 시대에 네트워킹의 복잡성과 제약을 없애고 고객과 파트너가 일상적으로 직면하는 가장 어려운 과제들을 해결해 나가고 있습니다. 주니퍼 네트웍스는 네트워크가 세상을 변화시키는 정보와 인재의 발전을 공유하는 근간이 되는 자원이라고 믿습니다. 주니퍼는 혁신적이고 획기적인 방식으로 빠르게 변화하는 비즈니스의 속도에 맞추어 확장 가능하고 자동화를 지원하는 안전한 네트워크를 제공할 것을 약속합니다.

본사
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
전화: 888.JUNIPER(888.586.4737)
또는 +1.408.745.2000
팩스: +1.408.745.2100
www.juniper.net

한국주니퍼네트웍스
서울 강남구 테헤란로 142
캐피탈타워 19층
우편번호 06236
www.kr.juniper.net
전화: 02-3483-3400
팩스: 02-3483-3488

JUNIPER NETWORKS | Engineering Simplicity