데이터 시트

A10 Defend DDoS Mitigator

지능형 자동화를 통한 DDoS 완화

A10 Defend DDoS Mitigator(구 Thunder TPS)는 A10 Defend 제품군 중 하나로 정밀도, 확장성 및 성능 면에서 업계를 선도하는 고급 머신 러닝으로 구동되는 확장 가능하고 자동화된 DDoS 방어 솔루션입니다.

정확한 다중 벡터 DDoS 방어

비즈니스 서비스의 가용성을 보장하기 위해 기업은 공격자와 합법적인 사용자를 정확하게 구별할 수 있는 확장 가능한 DDoS 방어를 구축하는 방법을 재고해야 합니다.

새로운 위협 벡터는 공격자가 사용할 수 있는 옵션의 폭, 강도 및 복잡성을 변화시켰습니다. 오늘날의 공격은 진화되어 이제 DDoS 툴 키트, 무기화된 IoT 장치, 온라인 DDoS 서비스 등을 포함합니다. 비효율적인 서명 기반 IPS 또는 트래픽 속도 제한에만 의존하는 기존의 솔루션은 더 이상 적절하지 않습니다.

DDoS 공격의 복잡성과 규모가 증가함에 따라 DDoS 보호 또한 발전하게 되었습니다. 전방위적인 DDoS 보호 제품군이 필요합니다. A10 Defend 제품군 중 하나로 뛰어난 정밀성을 갖춘 지능형의 확장 가능하고 자동화된 DDoS 완화입니다.

DDoS Mitigator는 사물 DDoS 및 기존의 좀비 봇넷을 방어하도록 확장하고, 반사 및 제로 데이 공격을 포함한 다중 벡터 DDoS 공격을 정밀하게 차단해 사용자에 대한 부수적 피해를 최소화합니다. 대규모로 자동 업데이트되는 위협 인텔리전스 목록, 5단계 적응형 완화 정책, 머신 러닝에 의해 구동되는 자동화된 제로 데이 공격 패턴 인식 등 지능형 자동화를 염두에 두고 고유한 다중 모드 및 소스 기반 보호 상태로 구축되었습니다.

Defend Orchestrator를 갖춘 DDoS Mitigator의 규모와 제로 터치 지능형 자동화 아키텍처는 제한된 직원으로도 효율성을 극대화하고 운영 비용을 줄여 ROI를 향상시킵니다. 따라서 A10 Defend DDoS Detector, DDoS Mitigator, Orchestrator 및 Threat Control로 구성된 A10 Defend 제품군은 조직이 보다 효과적으로 DDoS를 방어하거나 고객을 위해 수익성 있는 DDoS 스크러빙 서비스를 생성하는 데 도움이 됩니다.

A10 Networks는 도움이 가장 필요할 때 도움을 줍니다. A10 지원은 DDoS 사고를 즉시 이해하고 대응할 수 있도록 A10 DDoS 보안 사고 대응 팀(DSIRT)의 긴급 지원을 포함해 24x7x365 서비스를 제공합니다.

플랫폼

물리적 및 SPE 어플라이언스

가상 애플리케이션

클라우드

관련 제품 및 서비스

A10 Defend DDoS Detector

A10 Defend Orchestrator

A10 Defend Threat Control

DSIRT 지원

A10에 문의

A10Networks.com/a10-defend

이점

유지

서비스 가용성 유지

다운타임은 모든 비즈니스에서 즉각적인 생산성 및 수익 손실을 초래합니다. DDoS Mitigator는 트래픽 스펙트럼 전체에서 이상을 자동으로 감지하고 다중 벡터 DDoS 공격을 완화하여 서비스 가용성을 보장합니다.

차단

증가하는 공격 차단

DDoS Mitigator는 가장 크고 까다로운 네트워크 환경을 보호합니다. Defend Mitigator는 일반 공격 벡터를 특화된 하드웨어로 오프로드하여 강력한 멀티코어 CPU를 통해 합법적인 사용자와 공격 봇넷, 리소스 집약적인 심층 패킷 검사(DPI)가 필요한 복잡한 애플리케이션 계층 공격을 구별합니다.

확장 가능한

보호

엄선된 DDoS Mitigator 하드웨어 모델은 당사의 보안 및 정책 엔진(SPE) 하드웨어 가속을 통해 FPGA 기반 FTA 기술 및 기타 하드웨어에 최적화된 보안 검사를 활용하여 확장성이 뛰어난 패킷 처리 및 하드웨어 DDoS 방어 기능을 제공합니다. DDoS Mitigator 어플라이언스는 클러스터링 및 동기화 기술을 통해 하드웨어 또는 가상 어플라이언스 등 폼 팩터에 관계없이 완화 용량을 최대 8배까지 확장할 수 있습니다.

구축

전시 지원 구축

실시간 DDoS 공격에 대응할 수 있는 교육받은 직원이나 인력을 무제한으로 보유한 조직은 없습니다. DDoS Mitigator는 보호 영역당 5레벨의 프로그램 완화 확대 및 축소를 지원합니다. 일선 직원이 완화 전략 확대를 위해 시간이 오래 걸리는 수동 변경을 수행할 필요가 없으며, 공격 시 대응 시간을 단축할 수 있습니다. 관리자는 공격의 모든 단계에서 수동으로 개입하고 A10의 DSIRT과 협력할 수 있습니다.

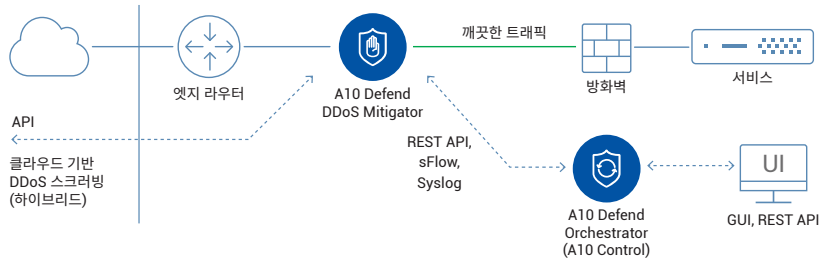
운영 비용

보안 운영 비용 절감

DDoS Mitigator는 매우 효율적입니다. 작은 폼팩터에 고성능을 제공하여 전력 사용량, 랙 공간 및 냉각 요구 사항을 크게 줄여 운영 비용을 절감합니다. DDoS Mitigator의 규모와 지능형 자동 완화 아키텍처는 A10 Defend Orchestrator와 함께 전체 DDoS 보호 워크플로와 탐지, 완화부터 보고까지의 라이프사이클을 단순화하는 동시에 보안 태세를 강화합니다.

A10 Defend 솔루션은 SecOps 팀의 효율성을 극대화하고 운영 비용을 줄여 ROI를 향상시킵니다.

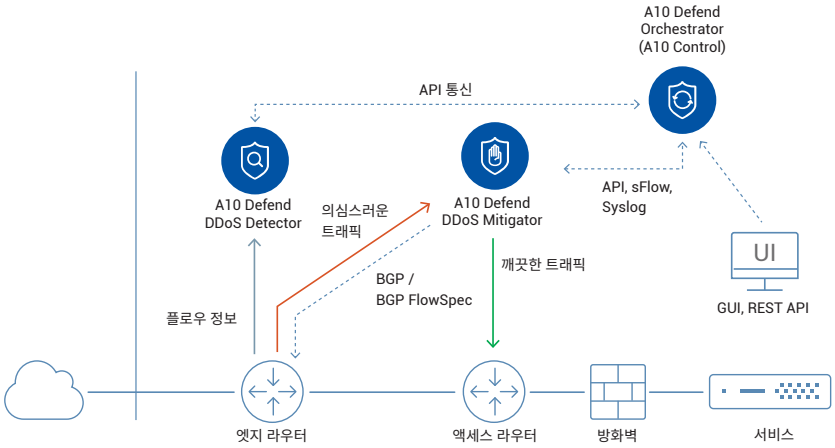
레퍼런스 아키텍처



사전 예방적 구축

(비대칭 또는 대칭)

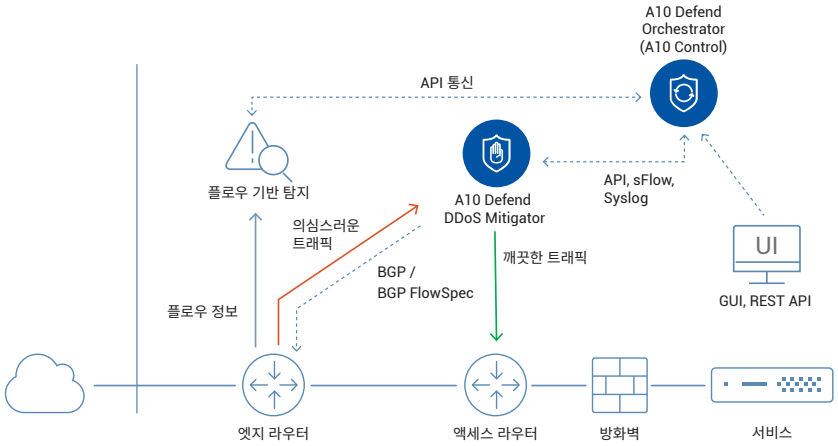
A10 Defend DDoS Mitigator를 서비스 네트워크 인라인 또는 경로 내에 배포하면 지속적이고 포괄적인 탐지 및 빠른 완화를 제공할 수 있습니다. 이 모드는 사용자 경험이 중요한 게임 및 VoIP와 같은 실시간 서비스와 애플리케이션 계층 공격에 대한 방어에 가장 유용합니다. DDoS Mitigator는 L2 또는 L3 경로 배포를 지원합니다. 또한 볼륨 공격이 조직의 인터넷 대역폭을 초과하는 경우, 클라우드 스크러빙 서비스와 함께 하이브리드 DDoS 방어를 쉽게 구축할 수 있습니다.



사후 대응적 구축

대규모 네트워크는 수동 또는 플로우 분석 시스템에 의해 트리거되는 주문형 완화의 혜택을 받을 수 있습니다. A10 Defend DDoS Detector는 독립형 어플라이언스(하드웨어 또는 가상)로 사용할 수 있습니다. 플로우 기반 DDoS 탐지기는 지능적이고 자동화된 DDoS 방어 솔루션을 위해 A10 Defend Orchestrator 및 DDoS Mitigator와 긴밀하게 통합됩니다. DDoS Mitigator는 업스트림 라우터와의 더 나은 협업을 위해 BGP FlowSpec을 보낼 수 있습니다.

레퍼런스 아키텍처



타사 플로우 탐지기를 사용한 사후 대응적 구축

A10 Defend DDoS Mitigator는 BGP 및 기타 라우팅 프로토콜 통합을 통해 모든 네트워크 구성을 지원합니다. 따라서 추가적인 전환과 리인젝션 라우터가 필요하지 않습니다. A10 Networks는 업계 선도적인 네트워크 모니터링 DDoS 탐지 회사와 협력하여 각 고객의 고유한 비즈니스 요구를 충족하는 동급 최고의 솔루션을 구축할 수 있는 탁월한 유연성을 제공합니다. 타사의 DDoS 탐지 기능은 API(A10의 aXAPI® 및 aGAPI®), syslog 또는 BGP Flowspec을 활용하여 긴밀하게 통합된 DDoS 방어 솔루션을 구축할 수 있습니다.

기능

풀 스펙트럼 DDoS 방어로 서비스 가용성 보장

완전한 솔루션

유연한 구축 지원

DDoS Mitigator는 사전 예방적 상시(Always-on) 모드 또는 주문형 사후 대응 모드로 DDoS 방어를 위한 완벽한 솔루션을 제공하여 고객의 비즈니스 목표를 충족합니다. 완전한 IPv4 및 IPv6 지원을 통해 L2 또는 L3에서 인라인 모드로 배포할 수 있습니다. 이때 사전 예방 모드는 게임, 음성 및 DNS와 같은 중요한 실시간 서비스에 적합합니다. 반응 모드에서 DDoS Mitigator는 DDoS Detector 및 Orchestrator와 함께 작동하며 필요할 때만 활성화됩니다. Detector가 공격을 탐지하면 Orchestrator는 Mitigator에 의심스러운 트래픽에 대한 BGP 경로 리디렉션을 시작하도록 지시합니다. 그러면 Mitigator는 깨끗한 트래픽을 의도한 목적지로 전달하기 전에 점진적인 자동 완화 수준 확대 기법을 사용하여 적절한 대응 조치를 적용합니다.

다중 벡터

공격 방어

볼륨, 프로토콜, 리소스 공격, 애플리케이션 수준 공격 또는 IoT 기반 공격 등 다양한 유형의 DDoS 공격을 완화시킵니다. 하드웨어 가속은 CPU를 오프로드하고 DDoS Mitigator가 동시 다중 벡터 공격을 능숙하게 처리할 수 있게 합니다.

하이브리드

DDoS 방어

DDoS Mitigator의 온프레미스 보호는 타사 클라우드 기반 DDoS 스크러빙 서비스와 함께 작동하여 모든 유형의 공격에 대한 풀 스펙트럼 방어를 제공합니다.

공격이 조직의 대역폭 용량을 초과하면 Mitigator는 BGP 기반 신호, API 및 스크립팅 등을 사용하여 자동으로 클라우드 완화를 시작할 수 있습니다.

ZAP

제로 데이 자동 방어

제로 데이 자동 방어(ZAP)는 휴리스틱 및 머신 러닝을 활용하여 고급 구성이나 수동 개입 없이 자동으로 완화 필터를 찾습니다. ZAP은 갈수록 정교해지는 다중 벡터 공격에 대한 응답 시간을 단축할 뿐만 아니라 다운타임과 오류를 최소화하고 운영 비용을 절감합니다.

논스톱 DNS

DNS 인증 캐시

DDoS Mitigator를 고성능 인증 DNS 캐시로 구성하여 Mitigator의 논스톱 DNS 운영 모드는 영역 전송을 이용해 최대 2억 4천만 개의 DNS 기록을 캐시하고 초당 최대 3,500만 개의 속도로 쿼리에 응답할 수 있습니다. 논스톱 DNS는 A10 Defend Mitigator DDoS 방어와 함께 작동하여 복원력이 뛰어난 DNS 서비스를 만들 수도 있습니다.

A10 DDoS 위협 인텔리전스

40개 이상의 신뢰할 수 있는 데이터 소스에서 집계된 상관관계가 있는 DDoS 무기 정보가 지원 기능에 포함되어 있어 Mitigator는 알려진 악성 소스에 대한 트래픽을 즉시 인식하고 차단할 수 있습니다. 이 서비스에는 반사 증폭 공격과 심각한 IoT 봇넷 공격에 정기적으로 사용되는 DDoS 무기에 대한 최신의 정확한 IP 주소가 수백만 개 포함되어 있습니다.

증가하는 공격 규모에 대응하는 고성능 및 효율성

고성능

보호

엄선된 Mitigator 모델에는 고성능 FPGA 기반 유연한 트래픽 가속(FTA) 기술이 탑재되어 데이터 CPU가 관련되기 전에 하드웨어의 패킷 및 프로토콜 이상을 포함하여 최대 60개의 일반적인 공격 벡터를 초당 최대 5억 패킷(Mpps)까지 즉시 완화시킵니다. Mitigator는 100ms 간격만큼 매우 세분화된 트래픽 속도를 적용합니다.

동시

객체 보호

Mitigator는 전체 네트워크, 애플리케이션 및 서비스를 보호하기 위해 영역당 수천 개의 호스트, 서브넷 및 서비스를 포함하는 개별 보호 정책을 사용하여 최대 3,000개의 영역을 동시에 완화합니다. 동시 완화 규모를 통해 조직은 보호된 객체를 세부적으로 제어하고 수익성이 높은 DDoS 스크러빙 서비스를 만들 수 있습니다.

확장성

최고의 완화 용량

Mitigator는 전력 효율적이고 작은 폼 팩터 하드웨어에서 5~380Gbps까지 모든 규모의 공격으로부터 조직을 보호하는 솔루션을 제공합니다. 또한 기능 패리티가 있는 가상 어플라이언스로도 사용 가능하며 100Gbps 처리량을 제공합니다.

목록 동기화 기술을 통해 최대 8개의 어플라이언스(예: 하드웨어에서 4.4Tbps, 가상 어플라이언스에서 800Gbps)를 클러스터링하여 완화 용량을 쉽게 확장할 수 있습니다.

정밀성

공격의 대규모 완화

Mitigator는 27개 이상의 트래픽과 동작 지표를 추적하고 확대 프로토콜을 적용하여 공격자와 유효한 사용자를 정확하게 구별하여 최대 3억 5,000만 개의 동시 추적 세션을 적절하게 완화할 수 있습니다.

복잡한 애플리케이션 공격(예: HTTP, DNS 등)을 다수의 CPU 코어에 대한 고급 병렬 처리를 통해 완화하여 다중 벡터 공격에도 고성능 시스템 확장을 유지합니다.

A10 Defend DDoS Mitigator

8665S

수치로 보는 성능

4.8 Tbps 하드웨어 차단	550 Gbps 처리량	4.4 Tbps 클러스터 처리량	8x16M 위협 클래스 목록
400 GE 포트	820 Mpps 비정상 손실 (HW 지원)	60 하드웨어 완화	64K 객체 보호

대규모 위협

정보 클래스 목록

각각 최대 1,600만 개의 항목을 포함하는 8개의 목록을 정의하여 A10 Defend Threat Control과 같은 DDoS 위협 인텔리전스 소스의 데이터를 활용할 수 있습니다. 이러한 클래스 목록은 자체 사용자 지정 블랙/화이트 리스트와 함께 IP 차단 목록으로 구성하거나 필요에 따라 소스 IP 기반 완화 정책에 사용할 수 있습니다.

제로 데이

공격 패턴 인식

DDoS 공격자는 새로운 전략으로 다중 벡터 공격 무기고를 지속적으로 혁신합니다. DDoS Mitigator 제로 데이 패턴 인식(ZAPR) 엔진은 고급 구성이나 수동 개입 없이 DDoS 공격 특성을 자동으로 식별해 완화 필터를 동적으로 적용합니다.

신속한 방어를 위한 완전한 제어 및 스마트 자동화

효율적인

지능형 자동화

수동 개입을 위한 인력이나 시간을 무제한으로 보유한 조직은 없습니다. A10은 전체 보호 라이프사이클에 대한 머신 러닝을 통해 구현된 업계 최고의 지능형 자동화 기능을 제공합니다.

운영자가 보호할 네트워크를 정의하기만 하면 A10 방어는 모니터링되는 엔티티별 개별 학습된 탐지 임계값, 자동 트래픽 리디렉션 조정, 완화 및 확대 시작, 공격 패턴 필터 추출 및 적용 등 운영자가 사전 정의한 정책에 기반하여 나머지 작업을 수행합니다. 공격이 진정되면 네트워크와 방어는 평시 상태로 회복되며, 향후 분석을 위해 세부적인 보고서가 생성됩니다.

쉬운

네트워크 통합

DDoS Mitigator는 다양한 성능 옵션 및 유연한 구축 모델을 통해 MPLS를 포함한 모든 규모의 네트워크 아키텍처에 통합될 수 있습니다. A10 또한 100% 프로그래밍 가능한 A10의 RESTful API, aXAPI를 통해 타사의 탐지 솔루션과 민첩한 SecOps 워크플로우에 쉽게 통합될 수 있습니다.

Mitigator는 BGP Blackhole, Flowspec 기능과 같은 개방형 표준을 활용하여 모든 DDoS 탐지 및 DDoS 완화 지원 BGP 라우터 솔루션과 쉽게 통합됩니다. 개방형 API 및 네트워킹 표준을 통해 A10 위협 탐지 파트너, SDN 컨트롤러 및 기타 보안 제품 등 다른 장치와의 긴밀한 통합도 가능합니다.

효율적인

관리

Mitigator는 업계 표준 CLI, 온박스 GUI 및 A10 Defend Orchestrator 중앙 집중식 관리 시스템을 지원합니다. 높은 수준의 운영자는 CLI를 사용하여 문제를 쉽게 해결하고 오류를 수정할 수 있습니다. 직관적인 온박스 GUI를 통해 사용이 간편하고 기본적인 그래픽 보고가 가능합니다. Defend Orchestrator는 여러 Mitigator 및 Detector 장치에 대해 고급 보고, 완화 콘솔, 정책 시행을 갖춘 포괄적인 대시보드를 제공합니다.

A10 Defend DDoS Mitigator 물리적 어플라이언스 사양

DDoS Mitigator	Thunder 1060S*4	Thunder 3350-E	Thunder 5845-40G	Thunder 5845
완화 성능				
처리량 (소프트웨어 스크러빙)*1	5/10/20 Gbps	10 Gbps	40 Gbps	100 Gbps
하드웨어 차단	N/A	N/A	250 Gbps	250 Gbps
패킷 속도 (pps)*1	2.5/5/800만	600만	1,200만	2,500만
소프트웨어 기반 - SYN 인증 (pps)	2.5/5/800만	600만	1,200만	2,500만
하드웨어 기반 - 비정상 플러드 차단 (pps)	N/A	N/A	1억 2,500만	1억 2,500만
최대 동시 세션 (대칭 배치)	8/10/1,600만	800만	3,200만	4,800만
평균 지연 시간	15 µs	20 µs	50 µs	50 µs
최소 속도 실행 간격	100 ms	100 ms	100 ms	100 ms
DNS 인증 캐시 성능				
초당 DNS 쿼리 (qps)	N/A	N/A	1,000만	1,800만
네트워크 인터페이스				
1GE (BASE-T)	7	6	0	0
1GE Fiber (SFP)	0	2	0	0
10/1GE Fiber (SFP+/SFP)	4	8 + 4*3	48	48
25/10GE Fiber (SFP28/SFP+)	2	0	0	0
40GE Fiber (QSFP+)	0	0	0	0
100/40GE Fiber (QSFP28/QSFP+)	0	0	4	4
400 GE Fiber (QSFP-DD)	0	0	0	0
관리 포트	이더넷 관리 포트, RJ-45 콘솔 포트			
하드웨어 사양				
프로세서	Intel 통신 프로세서 20 코어*5	Intel Xeon 8 코어	Intel Xeon 18 코어*5	Intel Xeon 18 코어
메모리 (ECC RAM)	32 GB	16 GB	64 GB	64 GB
스토리지	SSD	SSD	SSD	SSD
하드웨어 가속	소프트웨어	소프트웨어	2 x FTA-4, SPE	2 x FTA-4, SPE
크기 (인치)	1.75 (H) x 17.5 (W) x 17(D)	1.75 (H) x 17.5 (W) x 18(D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
랙 유닛 (마운팅 가능)	1U	1U	1U	1U
무게	12 lbs	18 lbs	34.3 lbs	34.3 lbs
전원공급장치 (DC 옵션 제공)	듀얼 300W RPS	듀얼 750W RPS	듀얼 1500W RPS	듀얼 1500W RPS
	80 Plus Gold 효율, 100 - 240 VAC, 50 – 60 Hz	80 Plus Platinum 효율, 100-240 VAC, 50-60 Hz		
소비 전력 (표준/최대)*2	112W / 127W	151W / 205W	585W / 921W	585W / 921W
발열량(BTU/h) (표준/최대)*2	383 / 434	516 / 700	1,997 / 3,143	1,997 / 3,143
냉각 팬 (전면-후면 공기 흐름)	탈착식 팬	핫스왑 스마트 팬		
작동 환경	온도 0° - 40° C | 습도 5% - 95%			
규제 인증	FCC Class A, UL^, ICES, CE, UKCA, CB^, VCCI, BSMI^, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS
표준 보증	90일 하드웨어 및 소프트웨어			

A10 Defend DDoS Mitigator 물리적 어플라이언스 사양(계속)

DDoS Mitigator	Thunder 7445	Thunder 7655S	Thunder 8665S
완화 성능			
처리량 (소프트웨어 스크러빙)*1	220 Gbps	380 Gbps	550 Gbps
하드웨어 차단	500 Gbps	1.2 Tbps	4.8 Tbps
패킷 속도 (pps)*1	5,000만	1억	1억 2,000만
소프트웨어 기반 - SYN 인증 (pps)	5,000만	1억	1억 1,000만
하드웨어 기반 - 비정상 플러드 차단 (pps)	2억 5,000만	5억	8억 2,000만
최대 동시 세션 (대칭 배치)	6,400만	2억 5,600만	3억 5000만
평균 지연 시간	60 µs	40 µs	40 µs
최소 속도 실행 간격	100 ms	100 ms	100 ms
DNS 인증 캐시 성능			
초당 DNS 쿼리 (qps)	3,500만	N/A	N/A
네트워크 인터페이스			
1GE (BASE-T)	0	0	0
1GE Fiber (SFP)	0	0	0
10/1GE Fiber (SFP+/SFP)	48	0	0
25/10GE Fiber (SFP28/SFP+)	0	0	0
40GE Fiber (QSFP+)	0	0	0
100/40GE Fiber (QSFP28/QSFP+)	4	16	0
400 GE Fiber (QSFP-DD)	0	0	12
관리 포트	이더넷 관리 포트, RJ-45 콘솔 포트		2 x 이더넷 관리 포트, RJ-45 콘솔 포트
하드웨어 사양			
프로세서	2 x Intel Xeon 18 코어	2 x Intel Xeon 28 코어	2 x Intel Xeon 36 코어
메모리 (ECC RAM)	128 GB	384 GB	512 GB
스토리지	SSD	SSD	SSD
하드웨어 가속	3 x FTA-4, SPE	2 x FTA-5, SPE	3 x FTA-6 FPGA
크기 (인치)	1.75 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
랙 유닛 (마운팅 가능)	1U	1.5U	1.5U
무게	35.7 lbs	44.2 lbs	44.9 lbs
전원공급장치 (DC 옵션 제공)	듀얼 1500W RPS	듀얼 1500W RPS	듀얼 2500W RPS
	80 Plus Platinum 효율, 100-240 VAC, 50-60 Hz		
소비 전력 (표준/최대)*2	784W / 1,078W	1,121W / 1,300W	1,491W / 1,720W
발열량(BTU/h) (표준/최대)*2	2,676 / 3,679	3,826 / 4,436	5,088 / 5,869
냉각 팬 (전면-후면 공기 흐름)	핫스왑 스마트 팬		
작동 환경	온도 0° - 40° C | 습도 5% - 95%		
규제 인증	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, RCM | RoHS
표준 보증	90일 하드웨어 및 소프트웨어		

하드웨어 사양 및 성능 수치는 예고 없이 변경될 수 있으며, 구성 및 환경 조건에 따라 달라질 수 있습니다. 네트워크 인터페이스는 네트워크 신뢰성 및 안정성을 보장하기 위해 A10 Networks 공인 광/트랜시버 사용을 권장합니다.

*1 처리량 성능은 트래픽 전달 용량이며 DDoS 보호가 활성화된 유효 트래픽으로 측정됩니다
*2 기본 모델 기준 | *3 10Gbps 속도만 | *4 모듈형 라이센스로 다양한 용량으로 제공됩니다. 사양 및 숫자는 모듈형 라이센스 계층에 따라 다릅니다
*5 활성 CPU 코어 수는 모듈형 라이센스에 따라 달라질 수 있습니다. | ^ 인증 진행 중

A10 Defend DDoS Mitigator 소프트웨어 사양

A10 Defend DDoS Mitigator 가상 어플라이언스	
지원되는 하이퍼바이저	VMware ESXi 6.7 이상 (SR-IOV)
하드웨어 요구 사항	설치 가이드 참조
표준 보증	90일 소프트웨어

가상 어플라이언스 라이센스 및 규모 권장 사항

처리량	Lab/1/2/5 Gbps	40 Gbps*1	100 Gbps*1
vCPU	6	8	24
vRAM	16 GB	32 GB	64 GB
vDisk	60 GB	60 GB	100 GB
라이센스 유형	대역폭 라이센스 (인스턴스당)	FlexPool	FlexPool
하이퍼바이저	ESXi	ESXi	ESXi

*1 ACOS 6.0 및 그 이상에서 제공됩니다. NVIDIA Mellanox ConnectX-6 NIC(SR-IOV 지원)를 사용하여 ESXi 7.0에서 실행되는 Defend Mitigator로 테스트

클라우드용 A10 Defend DDoS Mitigator	Microsoft Azure
인스턴스당 라이센스	최대 5 Gbps
이미지 포맷	Microsoft VHD
라이센스	30일 평가판 라이센스 | BYOL FlexPool 라이센스

상세한 기능 목록

기능은 어플라이언스에 따라 다를 수 있습니다.

탐지/분석

- 인라인 패킷 기반 DDoS 탐지
- 25만 6천 개 이상 서버 및 서비스에 대한 개별 탐지 정책
- 수동 및 학습 임계값
- 프로토콜 이상 탐지
- IPinIP내 검사(예: 네트워킹, 캡슐화)
- 블랙/화이트 리스트
- 트래픽 지표 및 상위 토커
- 완화 콘솔
- 패킷 디버깅 툴
- Top-k insights(소스, 목적지)
- 아웃바운드 탐지
- 피해자 IP 식별

DDoS 위협 인텔리전스 목록

- 첫 번째 보호 계층으로 유해한 IP 주소를 사전에 차단하기 위한 대용량 클래스 목록
- 최대 9,600만 개의 활성 항목 - 각각 최대 1,600만 개를 포함하는 최대 8개의 목록
- 각 목록에 대해 조치 또는 완화 정책 정의 가능
- A10 Defend Threat Control의 ThreatSTOP 및 IP 차단 목록을 포함한 다양한 유형의 DDoS 위협 인텔리전스 피드 지원

제로 데이 자동 방어

- ZAPR: 머신러닝 기반 공격 패턴 인식 및 필터링
- TCP 진행 추적
- 제로 데이 공격 방지
- 사전 구성 또는 수동 개입 불필요
- 빠르고 자동화된 응답

리소스 공격 방어

- 단편화 공격
- Slowloris
- Slow GET/POST
- Long form submission
- SSL 재협상

애플리케이션 공격 방어

- 애플리케이션 인식 필터
- 정규식 필터(TCP/UDP/HTTP/SIP)
- HTTP 요청 속도 제한(URI별)
- DNS 요청 속도 제한(유형, FQDN, 라벨 개수별)
- SIP 요청 제한(유형별)
- 애플리케이션 잘못된 형식의 요청 검사(DNS/HTTP/SIP)
- DNS 도메인 목록
- HTTP/S 프로토콜 컴플라이언스
- 애플리케이션(DNS/HTTP/SIP) 플러드 방어
- 서명 기반 IPS
- QUIC 버전 제어 및 잘못된 형식의 헤더 검사
- 게임 트래픽에 대한 패킷 워터마킹(UDP)
- 암호화된 플러드 공격 방어

프로토콜 공격 방어

- 무효 패킷
- 비정상적인 TCP 플래그 조합(플래그 없음, SYN-FIN, SYN 플래그, LAND 공격)
- SYN-ACK 증폭 공격 방어
- IP 옵션
- 패킷 크기 확인(ping of death)
- POODLE 공격
- TCP/UDP/SSL/ICMP 플러드 방어
- 연결별 트래픽 제어

챌린지 기반 인증

- TCP SYN 쿠키, SYN 인증
- ACK 인증
- 스푸핑 탐지
- DNS 인증
- HTTP 챌린지

객체 보호

- 자동화된 탐지 및 완화를 위한 보호 영역
- 소스/대상 IP 주소/서브넷
- 소스 및 대상 IP 패어
- 대상 포트
- 소스 포트
- 프로토콜(예: HTTP, DNS, SIP, TCP, UDP, ICMP 등)
- 클래스 목록/지리적 위치
- 패시브 모드
- 아웃바운드 완화 대칭 배치

논스톱 DNS 솔루션

- 인증 DNS 캐시로 작동
- 스크러빙 센터의 A10 Defend Mitigator로 원활한 계층 보호
- DNS water torture(임의 하위 도메인) 공격 방어
- 선택적이고 사용자 정의 가능한 조치(응답/전달/삭제)

작업

- 패킷 캡처
- 스크립트 실행
- 손실
- TCP 리셋
- 동적 인증
- 블랙 리스트에 추가
- 화이트 리스트에 추가
- 로그
- 동시 연결 제한
- 연결 속도 제한
- 트래픽 속도 제한(pps/bps)
- 다른 장치로 전달
- 원격 트리거된 블랙 홀(RTBH)
- BGP Flowspec

관리

- 전용 on-box 관리 인터페이스(GUI, CLI, SSH, Telnet)
- 포괄적인 관리를 위한 aGalaxy
- SNMP, syslog, email alert
- REST API(aXAPI) 또는 SDK
- LDAP, TACACS+, RADIUS 지원
- 구성 가능한 제어 CPU

네트워킹 및 배치

- 사전 예방, 사후 대응, 비대칭, 대칭, 대역 외(TAP)
- 투명(L2), 라우팅(L3)
- 가상 와이어
- 라우팅: static routes, BGP4+, OSPF, OSPFv3, IS-IS
- 양방향 포워딩 탐지(BFD)
- VLAN(802.1Q)
- 트렁킹(802.1AX), LACP
- 액세스 제어 리스트(ACL)
- 네트워크 주소 변환(NAT)
- MPLS 트래픽 보호
- BGP 루트 인젝션,
- BGP FlowSpec
- IPinIP(소스 및 터미네이트)
- GRE 터널 인터페이스
- VXLAN

상세한 기능 목록 (계속)

원격 측정

- 풍부한 트래픽 및 DDoS 통계 카운터
- sFlow v5
- 플로우 기반 내보내기를 위한 사용자 지정 카운터 블록
- 고속 로깅
- CEF 로깅

고성능의 확장 가능한 플랫폼

- 고급 코어 운영체제(ACOS)
- 선형 애플리케이션 확장
- 데이터 평면의 ACOS
- 제어 평면의 Linux
- IPv6 기능 패리티
- 정책 실행을 위한 하드웨어 가속을 지원하는 보안 정책 엔진(SPE)*
- 고성능 하드웨어 차단*

통신사급 하드웨어*

- 고급 하드웨어 아키텍처
- 핫스왑 이중화 전원공급장치(AC 및 DC)
- 스마트 팬(핫스왑)
- 솔리드 스테이트 드라이브(SSD)
- 위변조 검출
- 40 GbE 및 100 GbE 포트

보안 및 성능 보장 인증*

- 공통 평가 기준 EAL 2+
- FIPS 140- 2 Level 2 컴플라이언스(A10 Defend Mitigator 14045)
- FIPS 140-1 Level 1 컴플라이언스(전체)

* 기능과 인증은 어플라이언스에 따라 다를 수 있습니다.

더 알아보기

A10 Networks 소개

문의
kr_sales-dl@a10networks.com

파트 번호: A10-DS-15136-KR-02 Dec 2024