

Thunder SSLi

암호화된 트래픽에 대한 실시간 가시성을 위한 TLS/SSL 암호 해독

포괄적인 TLS/SSL 암호 해독 솔루션인 A10 Thunder® SSL Insight®(SSLi®)는 모든 포트에 대한 트래픽의 암호를 해독하여 타사의 보안 장치가 성능 저하 없이 기업의 모든 트래픽을 분석할 수 있도록 합니다.

사각지대 제거

Thunder SSLi는 타사 보안 장치에서 TLS/SSL 암호화가 CPU 집약적인 암호 해독 및 암호화 기능을 오프로드함으로 인해 발생하는 사각지대를 제거하면서 개인 정보 보호 표준을 준수합니다.

전용 보안 장치는 네트워크 트래픽을 심층적으로 검사하고 분석하지만, 고속으로 트래픽을 암호 해독하고 암호화하도록 설계되지 않았습니다. 실제로, 많은 보안 제품에는 트래픽 암호를 해독하는 기능이 전혀 없습니다. 따라서 Thunder SSLi는 기존 보안 장치를 보강하고, 보안 인프라에 대한 투자를 보호하며, 제로 트러스트 전략을 더욱 강화할 수 있도록 도와줍니다.

Thunder SSLi는 트래픽의 암호를 해독하여 차세대 방화벽, 침입 방지 시스템(IPS), 지능형 위협 보안(ATP) 솔루션 등과 같은 하나 이상의 타사 보안 장치로 전달하여 보안 인프라의 성능을 향상시킵니다. Thunder SSLi는 트래픽을 재암호화하여 의도된 목적지로 전달합니다. 응답 트래픽도 같은 방식으로 검사합니다.

A10 Harmony 컨트롤러®는 멀티 사이트의 Thunder SSLi에 대한 운영과 관리를 간소화할 수 있습니다. 포괄적인 대시보드를 제공하는 Harmony 컨트롤러는 네트워크 트래픽 특성에 대한 실시간 실행 가능한 통찰과 서비스, 애플리케이션 유형, URL 카테고리 등에 기반한 풍부한 분석을 제공하여 제로 트러스트 전략 강화에 필요한 가시성과 제어를 구현합니다.

플랫폼



다수의 클라우드 플랫폼



가상 애플리케이션



Dell OEM 솔루션
버드에 사용된 A10

관리



Harmony 컨트롤러
중앙 집중식 분석 및 관리

A10에 문의

A10networks.com/ssl

이점



한 번 암호 해독

여러 번 검사

A10의 SSL Insight 기술을 활용하여 SSL 트래픽의 암호를 해독하고 타사 보안 장치로 전달하여 검사합니다.

통합 로드 밸런싱과 컴퓨팅 집약적인 SSL 암호 해독에 대한 방화벽 및 기타 보안 장치의 부담을 덜어 업타임을 극대화하고 보안 인프라 용량을 늘려 공격 탐지 및 차단에 집중하게 합니다.



트래픽 암호 해독

모든 보안 장치 대상

기업 네트워크를 내부 및 외부 위협으로부터 보호하기 위해 조직은 다양한 보안 장치의 도움이 필요합니다.

Thunder SSLi는 주요 보안 공급업체와 협력하여 "보안 암호 해독 영역"에 다양한 방식으로 배치할 수 있어 전체 네트워크를 암호화된 위협으로부터 안전하게 보호합니다. Thunder SSLi의 연동성:

- 방화벽
- 보안 웹 게이트웨이(SWG)
- 침입 방지 시스템(IPS)
- 통합 위협 관리(UTM) 플랫폼
- 데이터 손실 방지(DLP) 제품
- 위협 방지 플랫폼
- 네트워크 포렌식 및 웹 모니터링 툴



운영 비용

절감

Thunder SSLi는 기업 트래픽의 암호를 해독하여 많은 인라인 및 비인라인 보안 장치로 전달하는 중앙 집중식 지점을 제공합니다. 이를 통해 각 보안 장치의 암호 해독 오버헤드를 제거하여 적절한 보안 주의를 유지하면서 성능을 향상시킵니다. 따라서 리소스를 많이 소모하는 암호 해독 및 암호화 기능을 지원하기 위해 더 큰 보안 장치를 구입할 필요가 없습니다.



완전한 가시성 확보로

사각지대 제거

Thunder SSLi는 모든 포트 및 다양한 프로토콜에서 트래픽의 암호를 해독하여 암호화 사각지대를 제거함으로써 보안 인프라가 이전에 보이지 않았던 트래픽을 검사하고 숨겨진 위협을 탐지해 방어할 수 있게 합니다.



인증서 상태

검증

공격자는 유효하지 않은 인증서를 사용해 네트워크에 침투할 수 있습니다. 이러한 공격을 차단하지 않으면 사용자는 여러 공격의 위협에 노출될 수 있습니다.

Thunder SSLi는 인증서 폐기 목록(CRL) 및 온라인 인증서 상태 프로토콜(OCSP)을 지원하여 시스템이 서버로부터 수신하는 인증서의 유효성을 확인할 수 있도록 지원합니다. 이를 통해 인증서가 유효한지 확인할 수 있습니다.



보장

컴플라이언스 및 개인 정보

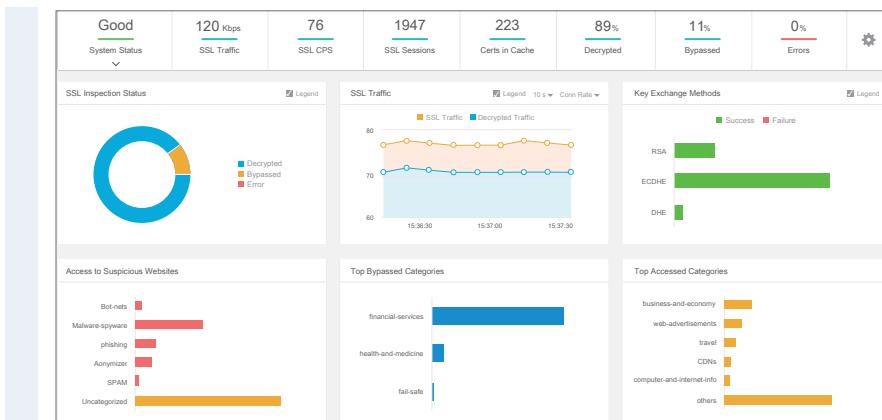
Thunder SSLi는 선택적 암호 해독을 지원하여 업계, 정부 및 기타 컴플라이언스 및 개인 정보 보호 표준을 준수할 수 있도록 보장합니다. 예를 들어, HIPAA 컴플라이언스는 개인 및 민감한 의료 정보의 암호 해독을 금지할 수 있습니다.



운영 및 관리

간소화

마법사 기반의 "직관적인" 구성, 배포 및 관리 툴인 AppCentric 템플릿은 Thunder SSLi를 업계에서 가장 사용하기 쉬운 암호 해독 솔루션으로 만듭니다. 정보를 제공하는 대시보드를 통해 네트워크를 쉽게 추적할 수 있습니다. Thunder SSLi에는 업계 표준 CLI, 웹 사용자 인터페이스 및 RESTful API(aXAPI[®])가 포함되어 있어 타사 또는 사용자 지정 관리 콘솔과 통합합니다.



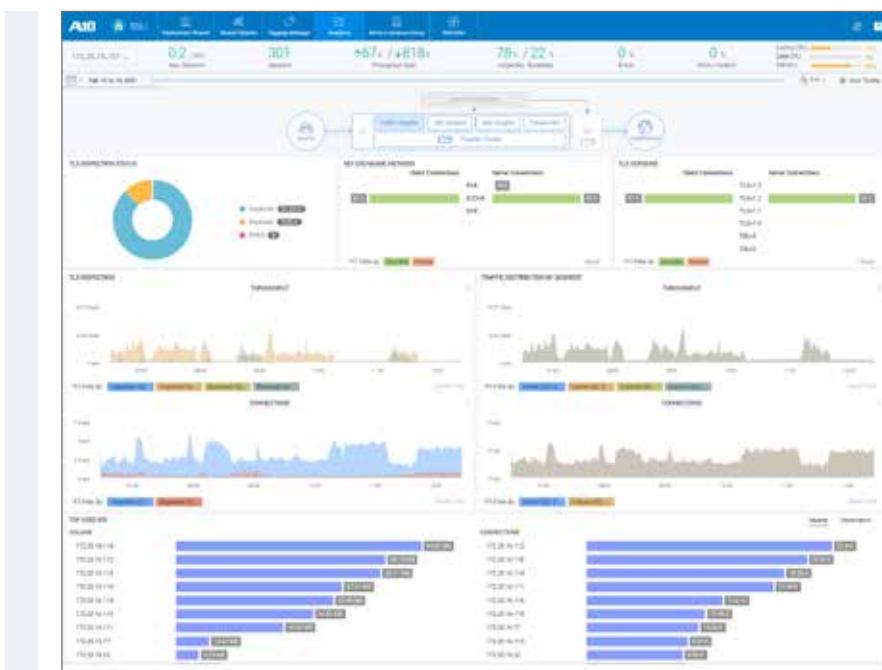
AppCentric 템플릿을 통해 사용자는 대시보드를 사용해 암호화된 트래픽을 관리하여 SSL 트래픽, 암호 해독 및 암호화, 우회, 분류를 사용한 트래픽 관리 등을 시각화할 수 있습니다.



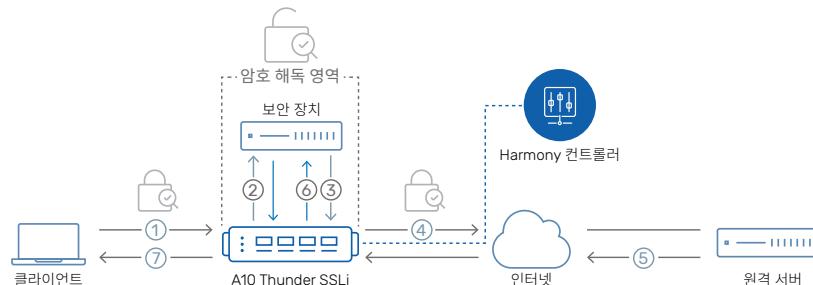
중앙 집중식

분석 및 관리

A10 Harmony 컨트롤러는 여러 지사의 여러 Thunder 장치에 대한 중앙 집중식 관리와 풍부한 분석 기능을 하나의 중앙 집중식 콘솔에 제공합니다. 배포된 Thunder 장치들을 중앙 위치에서 Harmony 컨트롤러를 통해 구성하고 관리할 수 있습니다. Harmony 컨트롤러는 개별 Thunder 장치 통계를 표시하거나 직관적인 대시보드에 통합하여 더욱 신속한 문제 해결 및 풍부한 분석을 제공할 수 있습니다.



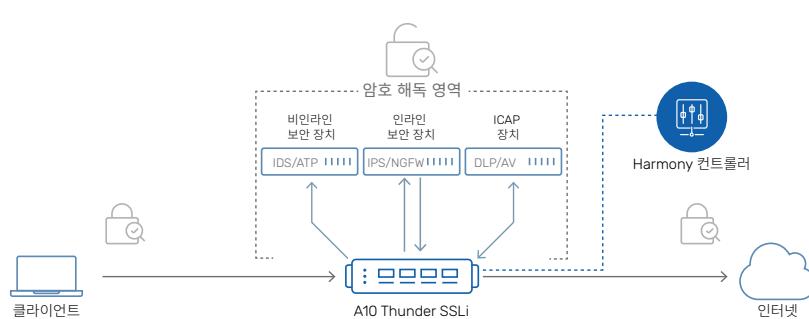
레퍼런스 아키텍처



- ① Thunder SSLi가 클라이언트의 암호화된 트래픽을 인터셉트해 암호를 해독합니다.
- ② Thunder SSLi가 암호를 해독한 트래픽을 보안 장치로 보냅니다.
- ③ 보안 장치가 일반 텍스트를 검사한 후 트래픽을 Thunder SSLi로 다시 보내 재암호화합니다.
- ④ Thunder SSLi가 재암호화한 트래픽을 서버로 보냅니다.
- ⑤ 서버는 요청을 처리하고 암호화된 응답을 Thunder SSLi로 보냅니다.
- ⑥ Thunder SSLi는 응답 트래픽의 암호를 해독하여 보안 장치로 보내 검사합니다.
- ⑦ Thunder SSLi가 보안 장치로부터 받은 트래픽을 재암호화하여 클라이언트로 보냅니다.

암호 해독 영역을 통한 트래픽 플로우

Thunder SSLi는 타사 보안 장치가 트래픽에서 위협을 검사하는 논리적 암호 해독 영역을 통해 가시성을 제공합니다. Thunder SSLi는 1대 또는 2대의 어플라이언스 구성으로 배포할 수 있습니다.



다중 배포 및 암호 해독 옵션

Thunder SSLi는 기업 경계에 인라인으로 배포할 수 있으며 인라인, 비인라인(패시브/TAP) 및 ICAP 지원 장치를 포함하는 다양한 보안 제품의 트래픽을 동시에 암호 해독할 수 있습니다.

Thunder 7655S SSLi

수치로 보는 성능

72 Gbps
SSLi 처리량

145 Gbps
SSLi 대량 처리량

4M
SSLi 동시 세션

100
GbE 포트



RSA: 100K
ECDHE: 70K
SSLi CPS

모든 보안 장치를 지원하는 트래픽 암호 해독 솔루션

방화벽

- Cisco FirePOWER
- Palo Alto Networks 차세대 방화벽
- Check Point 차세대 방어벽

보안 웹 게이트웨이

- Symantec Edge SWG
- Forcepoint Trusted Gateway System

지능형 위협 보안

- FireEye Network Security
- Fidelis Network

포렌식 및 보안 시스템

- RSA NetWitness
- IBM Security QRadar

침입 방지 시스템

- Trellix IPS (McAfee NSP)
- Secureworks iSensor

기타

- OPSWAT MetaDefender
- Trend Micro Deep Security
- Vectra NDR
- Garland Technology NPB
- Niagara Networks NPB/Bypass Switch

기능



암호 해독

여러 포트 및 프로토콜 검사

동적인 포트 검사를 통해 Thunder SSLi는 모든 TCP 포트에서 일반 TLS 트래픽의 암호를 해독합니다

STARTTLS, XMPP, SMTP, POP3과 같은 보안 서비스 프로토콜에 대한 암호 해독도 지원합니다. 암호 해독 기능은 SSL/TLS에만 국한되지 않으며, 암호화된 트래픽 및 SSH 트래픽에 대한 암호 해독도 지원합니다.



Full-proxy

아키텍처

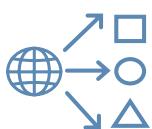
Thunder SSLi는 full-proxy로 작동하여, 암호화를 위한 Cipher suite 선택을 조정할 수 있습니다. Thunder SSLi는 유사한 강도의 다른 Cipher suite로 재협상할 수 있기 때문에, 향후 네트워크에 예고 없이 적용될 수 있는 새로운 암호 또는 TLS 버전에 대비할 수 있습니다. Thunder SSLi는 가장 안전한 암호를 사용하여 트래픽을 암호화하기 때문에 손상된 암호를 사용할 필요가 없습니다.



다중 암호

PFS 지원

Thunder SSLi는 전용 SSL 가속 하드웨어를 통해 2048비트 및 4096비트 키 크기로 고성능을 구현하고 DHE, ECDHE, ECDSA, ChaCha-Poly 등의 고급 Cipher suite를 지원하여 완전 순방향 비밀성(PFS)을 지원합니다.



선택적 암호 해독을 위한

URL 분류

Thunder SSLi URL 분류는 10억 개 이상 도메인의 트래픽을 카테고리로 분류하여 HIPAA와 같은 컴플라이언스 표준에 따라 개인 정보 보호 정책을 시행하기 위해 개인 정보/민감한 데이터(예: 의료 또는 재무 기록)의 암호가 해독되지 않도록 트래픽 암호 해독을 선택적으로 우회합니다.



액세스 제어를 위한

URL 필터링

URL 필터링을 사용해 악성 코드, 스팸, 피싱 소스 등 악의적인 웹사이트에 대한 액세스를 차단하여 직원의 생산성을 극대화하고 위험을 줄입니다.



부하 분산

보안 장치

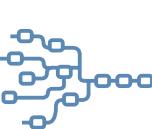
Thunder SSLi는 로드 밸런싱을 통해 방화벽 및 기타 보안 장치의 성능을 크게 향상시킵니다. 보안 용량을 쉽게 추가하고 기존 보안 장치의 수명을 연장합니다. 유연한 가중 트래픽 우선순위를 할당할 수 있습니다.



명시적 프록시

배포 지원

Thunder SSLi는 표준의 투명 프록시 배포 외에도 명시적 프록시로 배포할 수 있어 트래픽 관리에 대한 더 많은 제어 방식을 제공합니다. Thunder SSLi는 프록시 체이닝을 사용하여 여러 업스트림 프록시 서버에 연결할 수 있습니다.



애플리케이션 트래픽

인식 및 제어

애플리케이션 레벨에서 트래픽을 식별하고 분류하여 애플리케이션 가시성과 제어를 통해 세분화된 제어 및 정책을 정의할 수 있습니다. 이는 포괄적인 사용자 및 그룹 인식 기능과 함께 애플리케이션 트래픽을 더욱 심층적으로 파악할 수 있어 허용된 비즈니스 애플리케이션에 대한 효과적인 보안 계획을 세우고 제재할 수 있습니다.



ICAP

지원

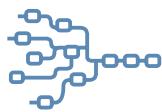
데이터 손실 방지(DLP) 시스템은 일반적으로 ICAP를 사용하여 네트워크에 연결하여 무단 데이터 유출을 방지합니다. Thunder SSLi는 다른 암호 해독 모드와 동시에 ICAP 연결을 지원합니다. 따라서 추가적인 솔루션을 구입할 필요 없이 네트워크의 기존 DLP 시스템을 사용할 수 있습니다.



세분화된

트래픽 제어

A10 aFlex® 스크립팅을 사용하여 요청 DPI를 검사, 업데이트, 수정 또는 삭제합니다. 어떤 트래픽을 인터셉트해 타사 보안 장치로 전달하고, 어떤 트래픽을 의도된 목적지로 보내기 전에 삭제해야 하는지를 완전히 제어합니다.



지능형 서비스 체이닝

고성능 보안

세분화된 정책을 사용하여 애플리케이션 유형에 따라 트래픽을 서로 다른 서비스 체인으로 선택적으로 리디렉션합니다. Thunder SSLi는 한 번 암호 해독을 수행하고 여러 번 검사하는 방식으로 암호 해독과 암호화 작업을 통합하여 지연 및 잠재적인 병목 현상을 줄입니다.



위협 인텔리전스

IP 위협 인텔리전스 피드는 암호 해독 프로세스를 시작하기 전에도 알려진 불량 IP 주소로 나가거나 해당 주소에서 들어오는 트래픽을 식별하고 차단합니다.

Threat Investigator를 사용하여 위협 평판 및 신뢰 점수를 기반으로 웹사이트의 신뢰성을 탐색하고 확인합니다. 이 기능은 on-box AppCentric 템플릿과 Harmony 컨트롤러를 통해 액세스할 수 있습니다.



사용자 인증 및 사용자 기반 정책

무단 액세스가 허용되지 않도록 ID 및 액세스 관리 기능을 사용하여 사용자를 위한 보안 정책을 만들 수 있습니다. 이를 통해 사용자 ID 기반 트래픽 및 검사 정책을 정의하여 세분화된 제어를 유지할 수도 있습니다.



중앙 집중식 분석 및 관리

A10 Harmony 컨트롤러는 장치 상태, 로그 및 트래픽 패턴 분석을 통해 성능 모니터링과 빠른 문제 해결을 제공합니다.

기업은 이상 징후 및 위협에 대한 심층적인 통찰을 바탕으로 동작 분석을 통해 적응형 제어 및 정책 업데이트를 설정할 수 있습니다.

Thunder SSLi 물리적 어플라이언스 사양

성능	Thunder 1060S-10G SSLi	Thunder 1060S SSLi	Thunder 3350S SSLi	Thunder 4440S SSLi
SSLi 처리량	1 Gbps	2 Gbps	5.5 Gbps	8 Gbps
SSLi CPS	RSA: 2K ECDHE: 1.2K	RSA: 6K ECDHE: 4K	RSA: 20K ECDHE: 10K	RSA: 22K ECDHE: 10K
SSLi 동시 세션	50K	100K	300K	400K
SSL 대량 처리량 ¹	10 Gbps	15 Gbps	30 Gbps	25 Gbps
네트워크 인터페이스				
1GE (BASE-T)	7	7	6	0
1GE Fiber (SFP)	0	0	2	0
10/1GE Fiber (SFP+/SFP)	4	4	8 + 4 ²	24
25/10GE Fiber (SFP28/SFP+)	2	2	0	0
40GE Fiber (QSFP+)	0	0	0	4
100/40GE Fiber (QSFP28/QSFP+)	0	0	0	0
관리 포트	이더넷 관리 포트, RJ-45 콘솔 포트			이더넷 관리 포트, RJ-45 콘솔 포트, Lights Out 관리
하드웨어 사양				
프로세서	Intel 통신 프로세서 20 코어 [9 코어 활성]	Intel 통신 프로세서 20 코어	Intel Xeon 14 코어	Intel Xeon 6 코어
메모리 (ECC RAM)	32 GB [24 GB 활성]	32 GB	64 GB	32 GB
스토리지	SSD		SSD	SSD
하드웨어 가속	소프트웨어		소프트웨어	2 x FTA-4
TLS/SSL 보안 가속	하드웨어		하드웨어	하드웨어
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)
랙 유닛 (마운팅 가능)	1U		1U	1U
무게	12 lbs		18 lbs	32.5 lbs
전원공급장치 (DC 옵션 제공)	듀얼 300W RPS 80 Plus Platinum 효율, 100 - 240 VAC, 50 - 60 Hz		듀얼 750W RPS	듀얼 1100W RPS
소비 전력 (표준/최대) ²	112W / 127W		175W / 222W	360W / 445W
발열량(BTU/h) (표준/최대) ²	383 / 434		598 / 758	1,229 / 1,519
냉각 팬 (전면-후면 공기 흐름)	탈착식 팬		핫스왑 스마트 팬	핫스왑 스마트 팬
작동 환경	온도 0° - 40° C 습도 5% - 95%			
규제 인증	FCC Class A, UL ³ , ICES, CE, UKCA, CB ⁴ , VCCI, BSMI ⁵ , RCM RoHS		FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM RoHS, FIPS 140-2 ⁶	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM RoHS
표준 보증	90일 하드웨어 및 소프트웨어			

Thunder SSLi 물리적 어플라이언스 사양(계속)

성능	Thunder 5440S SSLi	Thunder 5840S SSLi	Thunder 5840-11S SSLi	Thunder 6655S SSLi
SSLi 처리량	16 Gbps	20 Gbps	25 Gbps	36 Gbps
SSLi CPS	RSA: 35K ECDHE: 20K	RSA: 50K ECDHE: 25K	RSA: 50K ECDHE: 28K	RSA: 50K ECDHE: 35K
SSLi 동시 세션	800K	100만	200만	200만
SSL 대량 처리량 ¹⁵	45 Gbps	55 Gbps	55 Gbps	72.5 Gbps
네트워크 인터페이스				
1GE (BASE-T)	0	0	0	0
1GE Fiber (SFP)	0	0	0	0
10/1GE Fiber (SFP+/SFP)	24	24	48	0
25/10GE Fiber (SFP28/SFP+)	0	0	0	0
40GE Fiber (QSFP+)	4	4	0	0
100/40GE Fiber (QSFP28/QSFP+)	0	0	4	16
관리 포트	이더넷 관리 포트, RJ-45 콘솔 포트, Lights Out 관리			
하드웨어 사양				
프로세서	Intel Xeon 12 코어	Intel Xeon 18 코어	Intel Xeon 18 코어	Intel Xeon 28 코어
메모리 (ECC RAM)	64 GB	64 GB	128 GB	192 GB
스토리지	SSD	SSD	SSD	SSD
하드웨어 가속	2 x FTA-4	2 x FTA-4	2 x FTA-4	FTA-5, SPE
TLS/SSL 보안 가속	하드웨어	하드웨어 (2 옵션)	하드웨어	하드웨어
크기 (인치)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
랙 유닛 (마운팅 가능)	1U	1U	1U	1.5U
무게	32.5 lbs	32.5 lbs	34.3 lbs	39 lbs
전원공급장치 (DC 옵션 제공)	듀얼 1100W RPS 80 Plus Platinum 효율, 100 - 240 VAC, 50 - 60 Hz	듀얼 1100W RPS	듀얼 1500W RPS	듀얼 1500W RPS
소비 전력 (표준/최대) ¹²	360W / 445W	375W / 470W	550W / 760W	667W / 856W
발열량(BTU/h) (표준/최대) ¹²	1,229 / 1,519	1,280 / 1,604	1,877 / 2,594	2,276 / 2,921
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, KCC, BSMI, RCM RoHS, FIPS 140-2 ¹⁶	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM RoHS, FIPS 140-2 ¹⁶	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM RoHS, FIPS 140-2 ¹⁶
표준 보증	90일 하드웨어 및 소프트웨어			

Thunder SSLi 물리적 어플라이언스 사양(계속)

성능	Thunder 7440S SSLi	Thunder 7440-11S SSLi	Thunder 7655S SSLi
SSLi 처리량	25 Gbps	25 Gbps	72 Gbps
SSLi CPS	RSA: 45K ECDHE: 20K	RSA: 45K ECDHE: 20K	RSA: 100K ECDHE: 70K
SSLi 동시 세션	200만	200만	400만
SSL 대량 처리량 ⁵	75 Gbps	75 Gbps	145 Gbps
네트워크 인터페이스			
1GE (BASE-T)	0	0	0
1GE Fiber (SFP)	0	0	0
10/1GE Fiber (SFP+/SFP)	48	48	0
25/10GE Fiber (SFP28/SFP+)	0	0	0
40GE Fiber (QSFP+)	4	0	0
100/40GE Fiber (QSFP28/QSFP+)	0	4	16
관리 포트	이더넷 관리 포트, RJ-45 콘솔 포트, Lights Out 관리		
하드웨어 사양			
프로세서	2 x Intel Xeon 18 코어	2 x Intel Xeon 18 코어	2 x Intel Xeon 28 코어
메모리 (ECC RAM)	128 GB	128 GB	384 GB
스토리지	SSD	SSD	SSD
하드웨어 가속	3 x FTA-4	3 x FTA-4	2 x FTA-5, SPE
TLS/SSL 보안 가속	하드웨어	하드웨어	하드웨어
크기 (인치)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
랙 유닛 (마운팅 가능)	1U	1U	1.5U
무게	36 lbs	37 lbs	44.2 lbs
전원공급장치 (DC 옵션 제공)	듀얼 1100W RPS 80 Plus Platinum 효율, 100 - 240 VAC, 50 - 60 Hz	듀얼 1500W RPS	듀얼 1500W RPS
소비 전력 (표준/최대) ²	690W / 820W	820W / 950W	1,121W / 1,3001W
발열량(BTU/h) (표준/최대) ²	2,355 / 2,798	2,798 / 3,242	3,826 / 4,436
냉각 팬 (전면-후면 공기 흐름)	한스왑 스마트 팬		
작동 환경	온도 0° - 40° C 습도 5% - 95%		
규제 인증	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM RoHS, FIPS 140-2 ⁴	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM RoHS, FIPS 140-2 ⁴
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.

모든 SSLi 제품은 CFW 라이센스로도 제공됩니다. SWG 사용 사례(예: 애플리케이션 인식 방화벽 및 IP 위협 인텔리전스)의 경우 CFW 제품 라인이 필요합니다.

*1단일 어플라이언스 SSLi 구축에서 최대 SSL 옵션으로 테스트 되었습니다. RSA 2K 키 암호 "TLS_RSA_WITH_AES_128_CBC_SHA256"은 RSA 사례에 사용되고, EC P-256 암호 "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256"은 ECDHE 사례에 사용됩니다.

*2 기본 모델 기준. 수치는 SSL 모델에 따라 달라집니다. | *3 옵션의 RPS 제공 | *4 10Gbps 속도만 | *5 최대 SSL 옵션의 총 SSL(트랜잭션) 용량 | ^ 인증 진행 중 | + FIPS 모델을 구매해야 합니다.

Dell Technologies OEM 솔루션 번들에 사용된 A10 Thunder 사양

싱글 서비스 플랫폼(SSP) 사양

SSP 범위는 A10의 클라우드 지원 소프트웨어와 특수 제작된 Dell Technologies 하드웨어, 그리고 A10의 확장된 기능 세트와 애플리케이션 딜리버리 컨트롤러(ADC), SSL Insight(SSLi) 및 통신사급 네트워킹(CGN) 솔루션을 제공할 수 있는 포괄적 라이센스³로 구성됩니다.

Thunder SSLi 성능 ^{1 2 3}	Dell Technologies R640		Dell Technologies R740	
	10GE NIC 모델	100GE NIC 모델	10GE NIC 모델	100GE NIC 모델
SSL Insight 처리량	8.5 Gbps	12.5 Gbps	16.5 Gbps	30 Gbps
SSL Insight CPS (RSA / ECDHE)	28.5K / 13.5K	28.5K / 14.5K	30K / 18.5K	30K / 18.5K
SSL Insight 동시 세션	300만	300만	300만	300만
네트워크 인터페이스				
1GE (BASE-T)	2	2	2	2
10/1GE Fiber (SFP+/SFP)	6	2	10	10
100/40GE Fiber (QSFP28/QSFP+)	0	2	0	4
하드웨어 사양				
프로세서	2 x Intel Xeon 20 코어		2 x Intel Xeon 20 코어	
메모리	192 GB		192 GB	
스토리지	2 x SSD		2 x SSD	
TLS/SSL 보안 프로세서	2 x 보안 카드 (PCIe)		2 x 듀얼 칩 보안 카드 (PCIe)	
전원공급장치	듀얼 750W 전원공급장치		듀얼 2000W 전원공급장치	

멀티 테넌트 가상 플랫폼(MVP) 사양

Dell Technologies에 사용된 A10 Thunder 멀티 테넌트 가상 플랫폼(MVP)은 단일 플랫폼에서 여러 개의 가상 인스턴스 또는 서비스를 지원하고 A10의 확장된 기능 세트와 함께 애플리케이션 딜리버리 컨트롤러(ADC), SSL Insight(SSLi) 및 통신사급 네트워킹(CGN) 솔루션을 제공할 수 있는 포괄적 라이센스²를 포함하는 고급 플랫폼입니다.

SSL Insight 사용 성능 ^{1 2 3}	Dell Technologies R640		Dell Technologies R740	
	10GE NIC 모델	100GE NIC 모델	10GE NIC 모델	100GE NIC 모델
SSL Insight 처리량	6.8 Gbps	15.5 Gbps	13.8 Gbps	32.5 Gbps
SSL Insight CPS (RSA / ECDHE)	12.5K / 7K	55K / 32K	27K / 14K	68.5K / 52.5K
SSL Insight 동시 세션	58K	680K	118K	680K
네트워크 인터페이스				
1 GE (BASE-T)	2	2	2	2
1/10 GE Fiber (SFP+)	6	2	10	10
100 GE Fiber (QSFP28)	0	2	0	4
하드웨어 사양				
프로세서	2 x Intel Xeon 20 코어		2 x Intel Xeon 20 코어	
메모리	192 GB		192 GB	
스토리지	2 x SSD		2 x SSD	
TLS/SSL 보안 프로세서	2 x 보안 카드 (PCIe)		2 x 듀얼 칩 보안 카드 (PCIe)	
전원공급장치	듀얼 750W 전원공급장치		듀얼 2000W 전원공급장치	

*1 SSLi 성능은 L3에서 듀얼 파티션 모드 배포로 RSA(2K 키) 암호 "TLS_RSA_WITH_AES_128_CBC_SHA" 및 ECDSA(EC P-256) 암호 "TLS ECDHE_RSA_WITH_AES_128_CBC_SHA"를 사용하여 테스트되었습니다.

*2 A10 Thunder의 Dell Technologies OEM 번들 솔루션은 CFW(Convergent Firewall) 라이센스에 따라 라이센스가 부여되었습니다. 전체 기능 테스트 및 검증에 대한 최신 정보는 A10 Networks 영업 담당자에게 문의해 주십시오.

*3 모든 Thunder MVP 성능 사양은 다음 VM 프로파일을 사용하는 총수입니다:

- R640 10GE NIC 모델은 1 VM, R740 10GE NIC 모델은 2 VM을 사용하여 테스트되었습니다. 각 vThunder에는 8 CPU, 16 GB 메모리, 30 GB 스토리지, 8 SSL VF가 할당되었습니다.

- R640 및 R740 100GE NIC 모델은 4-VM 프로파일(각 vThunder에 16 vCPU, 32 GB 메모리, 30 GB 스토리지, 16 SSL VF 할당)을 사용하여 테스트 되었습니다.

Thunder SSLi 가상 어플라이언스 사양

vThunder SSLi					
지원되는 하이퍼바이저	VMware ESXi (VMXNET3, SR-IOV, PCI Passthrough), KVM QEMU (VirtIO, OvS with DPDK, SR-IOV, PCI Passthrough), Microsoft Hyper-V ⁺				
하드웨어 요구 사항	설치 가이드 참조				
표준 보증	90일 소프트웨어				
대역폭 라이센스	Lab	200 Mbps	1 Gbps	4 Gbps	8 Gbps
VMware ESXi	●	●	●	●	●
KVM	●	●	●	●	●
Microsoft Hyper-V ⁺	●	●	●	●	●

+ Hyper-V는 ACOS 4.x 및 5.x 릴리스에서 지원됩니다. 8 Gbps 라이센스 권장되지 않음.

상세한 기능 목록

기능은 어플라이언스에 따라 다를 수 있습니다.

탐지/분석

- 순방향 프로토콜로 사용되는 고성능 SSL 암호 해독 및 암호화
- Full-proxy 아키텍처
- 데이터 손실 방지(DLP) 및 안티바이러스 솔루션을 위한 사전 필터링으로 인터넷 콘텐츠 적응 프로토콜(ICAP) 지원
- TCP 포트 번호와 상관 없이 SSL 또는 TLS 트래픽을 탐지하고 인터셉트하기 위한 동적 포트 암호 해독
- 들어오는 웹 위협을 차단하기 위해 양방향 검사
- 핸드셰이크 오류 시 트래픽을 우회하는 순방향 프록시 페일세이프
- 호스트 이름에 기반한 암호 해독 바이패스, 바이패스 목록 최대 100만 서버 이름 표시(SNI) 값까지 확장
- 멀티 우회 목록 지원
- 광범위한 암호 및 프로토콜 지원
 - SSL 3.0, TLS 1.0/1.1/1.2/1.3³
 - RSA/DHE/ECDHE/ECDSA/ChaCha-Poly 암호 및 완전 순방향 비밀성(PFS) 지원
 - SHA, SHA-2, MD5 메시지 인증 코드(MAC) 알고리즘
 - IPv4 및 IPv6
 - HTTP 1.1, HTTP/2
- HTTPS, STARTTLS, SMTP, XMPP, POP3, SSH, SCP, sFTP의 암호 해독
- 클라이언트 인증서 탐지 및 선택적 우회
- 다음을 사용하여 신뢰할 수 없는/만료된 인증서 처리:
 - 온라인 인증서 상태 프로토콜(OCSP)
 - 인증서 폐기 목록(CRL)
- 상세한 사용자 및 세션 로깅
- ID 기반 액세스 제어를 위한 사용자 인증 및 인증 서비스
- SaaS 로컬 브레이크아웃 및 액세스 제어
- 인터넷 트래픽 부하 분산 및 최적화를 위한 흡간 부하 분산(NHLD)
- SSLi 이벤트의 플로우 정보를 기록하는 TLS 알림 로깅
- SSL 세션 ID 재사용
- 사용자 정의 가능한 애플리케이션 인식 스위칭을 위한 aFlex 스크립팅
- 고가용성: active-active, active-standby 구성
- 방화벽 로드밸런싱(FWLB)

URL 분류²

- 웹 카테고리 기반 선택적 암호 해독을 위한 URL 우회
- 알려진 악의적이거나 바람직하지 않은 웹사이트 차단을 위한 URL 필터링

위협 인텔리전스²

- IP 위협 인텔리전스¹ 사용자 정의 가능한 위협 점수 및 허용 오차에 따라 악의적인 트래픽의 네트워크 유입 방지
- Threat investigator은 URL, IP, 앱 등과 같은 개체에 대한 풍부한 상황별 분석 제공.

애플리케이션 인식 방화벽^{1,2}

- 애플리케이션 내 서비스 유형 식별을 통한 수천 개의 프로토콜 서명 인식
- 실시간으로 실행하는 사용자 정의 규칙 지원

배포

- 인라인 투명 프록시 또는 비인라인 타사 장치로 명시적 프록시 배포
- 인라인 투명 프록시 또는 인라인 타사 장치로 명시적 프록시 배포
- 인라인 투명 프록시 또는 ICAP 연결 장치로 명시적 프록시 배포
- 인라인 투명 프록시 또는 프록시 챈팅을 사용하는 타사 투명 및 명시적 프록시 장치로 명시적 프록시 배포

가상화

- VMware vSphere ESXi, Microsoft Hyper-V 및 KVM용 vThunder 가상 어플라이언스
- Dell Technologies OEM 솔루션 번들에 사용된 A10 Thunder

관리

- 전용 on-box 관리 인터페이스(GUI, CLI, SSH, Telnet)
- 웹 기반 AppCentric 템플릿(ACT) 지원
- SNMP, syslog, email alert
- RESTful API(aXAPI)
- LDAP, TACACS+, RADIUS 지원
- 구성 가능한 제어 CPU
- 중앙 집중식 관리, 구성 및 분석을 위해 A10 Harmony 컨트롤러와 상호 운용 가능

Harmony 컨트롤러를 통한 중앙 집중식 관리 및 분석

- 멀티 사이트의 장치 및 구성 관리
- 구성을 안내하는 배포 마법사
- 중앙 집중식 보안 정책 관리 및 실행
- 트래픽, 애플리케이션, URL, 소스 및 목적지 등에 대한 통찰을 제공하는 풍부한 TLS/SSL 트래픽 및 암호 해독 분석
- Threat investigator 뷰
- 세부적인 세션 로그
- 문제 해결 툴

* 기능은 어플라이언스에 따라 다를 수 있습니다.

*1 CFW 플랫폼/라이센스에서 사용할 수 있습니다.

*2 소프트웨어 및 서비스 기입이 필요합니다.

*3 Thunder 3350S, 5840S(QSSL), 6655S 및 7655S에서 사용할 수 있습니다.

더 알아보기

A10 Networks 소개

문의

kr_sales-dl@a10networks.com

©2024 A10 Networks, Inc. All rights reserved. A10 Networks, A10 Networks 로고, ACOS, Thunder, Harmony, SSL Insight는 미국 및 기타 국가에서 A10 Networks, Inc.의 상표 또는 등록 상표입니다. 기타 모든 상표는 해당 소유자의 자산입니다. A10 Networks는 이 문서의 부정확성에 대해 책임을 지지 않습니다. A10 Networks는 예고 없이 이 긴행물을 변경, 수정, 전송, 개정할 수 있는 권리를 보유합니다. 상표 전체 목록을 확인하시려면 링크를 방문하십시오: A10Networks.com/a10trademarks.