데이터시트

고용량 회선 속도 암호화 모듈

6500 Packet-Optical Platform용

전송 중 데이터의 기밀성을 보장하도록 설계된 Ciena의 6500 Packet-Optical Platform은 프로토콜 제약이 없는 유연한 10G, 100G 또는 200G 회선 속도 암호화 솔루션을 비용 효과적으로 전달합니다. 이 암호화 솔루션은 쉬운 운영 및 관리와 같은 이점을 제공하여 이더넷, Fibre Channel, SONET/SDH 및 OTN(광 전송망) 서비스를 위한 데이터 보호 전략을 효율적으로 이행할 수 있도록 지원합니다.

Ciena의 WaveLogic Encryption 솔루션은 전 세계 거대 인프라에서 운용 중인 플랫폼에 이미 활용되고 있는 입증된 암호화 기술을 전 세계 600개 이상의 통신 사업자들이 운용하는 6500의 입증된 안정성과 결합했습니다. 통신 사업자들은 암호화 기술의 운용을 간소화하는 솔루션을 사용하는 것이 좋습니다. 이러한 솔루션은 암호화 기능을 전송 네트워크 내부에 있는 네워크 요소에 직접 통합하고 네트워크 복잡성을 감소시키며 다양한 애플리케이션에서 다양한 암호화 솔루션을 관리해야 하는 필요성을 제거합니다.

탁월한 보안성을 보유한 인증된 솔루션

암호화 기능은 네트워크에서 데이터의 기밀성, 무결성 및 가용성을 보장하는 Ciena 다중 계층 보안 접근법의 일부이며, Ciena의 WaveLogic Encryption 솔루션에 탑재되어 모든 트래픽을 상시 암호화함으로써 가장 높은 수준의 보안성을 보장합니다. 상황에 따라 암호화 기능을 켜거나 끄는 것이 유연하게 보일 수는 있지만 사람이 만드는 작은 오류로 인해 중요한 트래픽을 암호화되지 않은 네트워크로 보내버릴 수 있습니다. Ciena 솔루션은 외부에서 검증하고 제3자가 수행하는 독립적 인증 절차를 거침으로써 표준 기반 AES 엔진과 알고리즘으로 효과적으로 구현합니다. CC(Common Criteria) 및 FIPS 인증을 포함하여 가장 높은 수준의 보안 표준을 준수하는 이 솔루션은 표준 기반 인증 메카니즘 기술(예: X.509 인증)을 가진 FIPS 인증 AES-256 암호화 엔진을 제공하며, 이를 통해 기존 기업 PKI에 매끄럽게 통합하여 운영을 간소화합니다.

특징 및 장점

- 높은 수준의 보안성과 투명성을 가진 종단 간 통신을 위해 초저 지연 시간의 회선 속도 암호화 솔루션을 제공합니다.
- 프로토콜 제약이 없는 암호화 기술을 특징으로 하며 탁월한 유연성으로 다양한 서비스를 지원합니다.
- FIPS 인증 AES(Advanced Encryption Standard) 256 암호화 솔루션을 통해 전송 중인 중요 데이터 보안을 보장합니다.
- 인증 기능과 데이터 암호화 기능을 위한 2종의 개별 키 세트(초 단위로 빠르게 암호화 키 교대)를 활용합니다.
- X.509 인증서 기반 인증을 사용하여 기존 기업 PKI(Public Key Infrastructure)에 매끄럽게 통합됩니다.
- 통합된 관리 도구를 통해 통신사 관리형 또는 기업 관리형 인프라에서 최종 사용자가 EaaS(Encryption-as-a-Service) 기능을 안전하게 관리할 수 있습니다.
- 전 세계에서 운용 중인 금융, 공공기관, 의료, 군사 및 정부 기관 네트워크에서 널리 활용되고 현장에서 입증된 암호화 솔루션을 제공합니다.

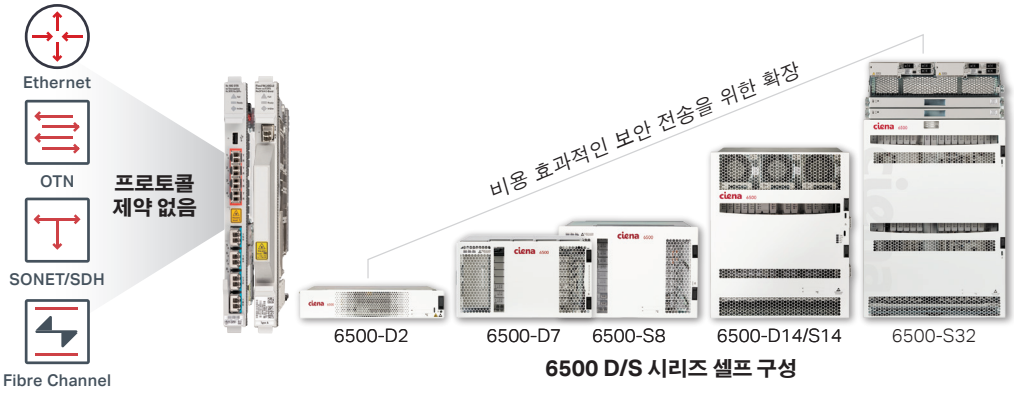

그림 1: 확장을 통해 네트워크 요구를 충족시키는 프로토콜 제약이 없는 6500용 WaveLogic Encryption 솔루션

전례 없는 수준의 유연성

6500의 뛰어난 유연성을 통해 고객은 사이트별로 다양한 용량, 공간 및 전력 요구에 적합한 최적 크기의 셸프를 선택함으로써 암호화 서비스를 비용 효과적으로 전달할 수 있습니다. 다른 중요한 이점은 프로토콜 제약이 전혀 없기 때문에 매우 다양한 클라이언트를 유연하게 지원하여 보안을 중요하게 고려하는 고객을 위해 다양한 애플리케이션 요구를 충족시킬 수 있습니다. 또한 이 솔루션을 활용하면 낮은 지연 시간 연결과 여러 경로/장비 보호 옵션으로 다양한 서비스를 운용할 수 있습니다.

Encryption Testing and Certification 인포브리프 다운로드

가장 견고한 암호화 기능

더 높은 수준의 보안을 위해 별개의 독립적인 2종의 키가 인증 기능과 데이터 암호화 기능을 위해 사용됩니다. 이때 분 단위가 아닌 초 단위 간격으로 빠르게 암호화 키가 교환됩니다.

그림 2. 암호화 모듈을 탑재한 4x10G OTR 모듈

AES-256 데이터 암호화 세션 키는 사용자의 간섭 없이 그리고 트래픽이나 처리량에 영향을 주지 않고 자체적으로 교섭되고 각 회선 포트에서 매 초마다 독립적으로 교환됩니다. 통신 사업자는 ECC(Elliptic Curve Cryptography)를 지원하는 차세대 공용 키 암호화 알고리즘을 활용할 수 있습니다. ECC는 1세대 공용 키 암호화 시스템보다 훨씬 뛰어난 보안화 전략을 제공합니다.

10G 회선 속도 암호화

통신 사업자는 프로토콜 독립적인 암호화 회선 포트 4개를 통해 40G 회선 속도 암호화 서비스를 지원하는 암호화 모듈과 함께 단일 슬롯 4x10G OTR(Optical Transponder)을 활용하여 10G 암호화 서비스를 비용 효과적으로 제공할 수 있습니다. 이 FIPS 140-2 Level 3 호환 모듈은 초기화를 통해 물리적 탬퍼링(악용 및 변조)으로부터 중요 정보를 안전하게 보호합니다. 즉 암호화 모듈이 셸프에 연결되어 있지 않은 경우에도 모듈에서 물리적 탬퍼링이 감지되는 순간 모든 데이터를 영(0)으로 설정합니다.

프로그래밍 가능 100G 또는 200G WaveLogic Encryption

Ciena의 WaveLogic Encryption 솔루션은 산업을 선도하는 WaveLogic 코히어런트 기술을 활용하며 새로운 WL3 (WaveLogic 3) Extreme 회선 모듈을 통해 유연하고 맞춤 가능한 고용량 암호화 솔루션을 구현하도록 지원합니다. WL3 Extreme은 WL3의 기능을 기반으로 개발되었으며, 추가적인 변조 기술을 사용하고 선형 및 비선형 장애를 개선하는 기능을 통해 모든 코히어런트 네트워킹 애플리케이션에 최고의 성능을 제공합니다.

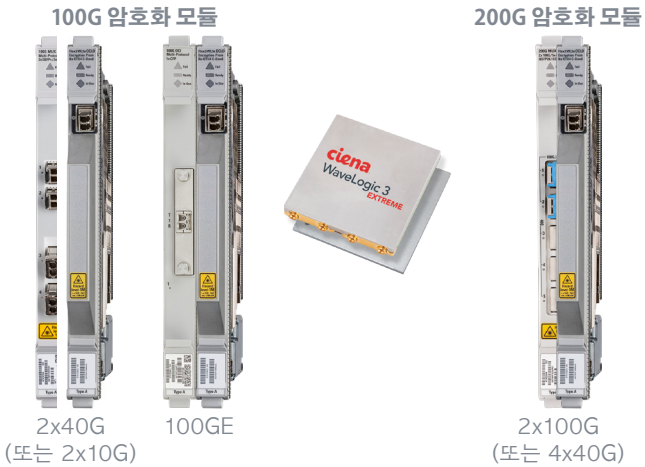

그림 3. 프로그래밍 가능한 100G 또는 200G 회선 속도 암호화 모듈과 WL3 Extreme 회선 모듈의 예

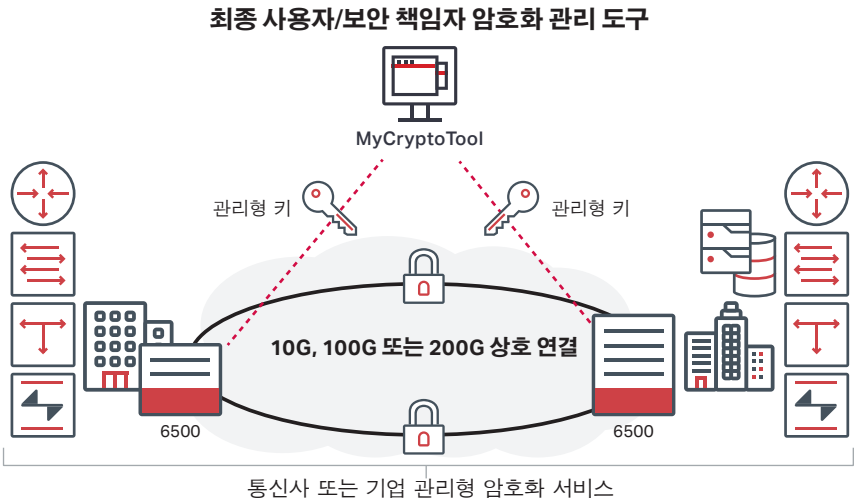

그림 4. MyCryptoTool 전용 암호화 관리 인터페이스

Data Security with Optical Encryption 인포그래픽 다운로드

이 최첨단 솔루션은 메트로에서 장거리까지 모든 인프라 요구 사항을 해결하며, 소프트웨어 프로그래밍 변조 기술을 제공하여 QPSK 변조를 사용하는 100G 암호화 기능과 업계 최초로 16QAM 변조를 사용하는 200G 암호화 기능 모두를 지원합니다.

통신 사업자는 이 WL3 Extreme 회선 모듈을 다양한 클리어언트 인터페이스와 통합함으로써 특정 트래픽 요구(10G, 40G 또는 100G 서비스 전송)를 효과적으로 충족시키는 맞춤형 솔루션을 유연하게 운용할 수 있습니다. 트래픽 수요가 증가하면 추가 클라이언트 카드를 연결하여 200G의 암호화 트래픽을 전송하도록 동일한 WL3 Extreme 회선 모듈을 프로그래밍할 수 있습니다. 뿐만 아니라 6500의 고용량 하이브리드 패킷/OTN 패브릭을 활용하여 고용량 암호화 서비스를 네트워크 전반에서 운용할 수 있어 네트워크 리소스 효율성을 극대화할 수 있습니다.

간소화된 암호화 관리

Ciena의 WaveLogic Encryption 솔루션은 분산 네트워크 관리를 위해 설계된 전용 암호화 관리 인터페이스인 MyCryptoTool을 통합하고 있습니다. 이 도구를 사용하는 최종 사용자와 보안 책임자는 10G, 100G 또는 200G 통신사 관리형 서비스나 기업 관리형 서비스의 보안 매개 변수와 경보를 독립적으로 관리할 수 있습니다. MyCryptoTool은 사용자 친화적인 인터페이스이며 암호화 모듈에 대한 보안 연결을 구성하고 상호 인증을 제공하여 인증된 보안 사용자로만 액세스를 제한합니다.

Ciena의 WaveLogic Encryption 솔루션은 탁월한 유연성과 보안성 이점을 쉬운 운영과 관리에 결합함으로써 프로토콜 제약이 없고 비용 효과적인 10G/100G/200G 초저 지연 시간 암호화 솔루션을 구현하며 그 결과로 사실상 오늘날의 모든 웹스케일 통신 애플리케이션의 보안 수준을 한 차원 높입니다.

Wire-speed Encryption Solution 애플리케이션 정보 다운로드

기술 정보

회선 팩	암호화 기능을 탑재한 4x10G OTR	암호화 기능을 갖춘 WaveLogic 3 Extreme 회선 모듈
시스템 요구 사항	모든 6500 S/D 시리즈 새시에서 운용	6500-D2를 제외한 모든 6500 S/D 시리즈 새시에서 운용
포트 형식 **클라이언트 지원 인터페이스**	OC-192/STM-64 10GbE LAN, 10GbE WAN FC400, FC800, FC1200 OTU2, OTU2e	OC-192/STM-64 10GbE LAN, 10GbE WAN, 40GbE, 100GbE FC800, FC1200 OTU2, OTU2e, OTU3, OTU4, ODU-Flex
회선 지원 인터페이스	OTU2 OTU2e	코히어런트 100G(QPSK): 1xOTU4 코히어런트 200G(16QAM): 2xOTU4
보호 옵션	1+1 회선 보호 1+1 클라이언트 및 장비 보호	1+1 회선 보호 1+1 클라이언트 및 장비 보호
FEC 모드	G.709 준수 RS-8 FEC, UFEC 및 OFF	연판정 FEC
환경 특성 작동 온도 상대 습도 고도	 +5° C ~ +40° C(+41° F ~ +104° F) -5° C ~ +55° C(+23° F ~ +131° F) 단기 – 6500-D2/D7/S8/D14/S14 -5° C ~ +50° C(+23° F ~ +122° F) 단기 – 6500-S32 5% ~ 85%(비응축) 4,000m (13,000피트)	
물리적 특성	11.34인치(H) x 0.99인치(W) x 9.34인치(D) 288mm(H) x 25mm(W) x 237mm(D)	
보안 기능	• 데이터 암호화를 위한 NIST 인증 AES-256 암호화 솔루션 • ECC(Elliptic Curve Cryptography) 알고리즘 • Diffie-Hellman 보안 키 교섭(Elliptic Curve 포함) • 인증을 위한 X.509 인증서 지원 • CRL(Certificate Revocation List) 지원 • 무중단 AES-256 키 교대(초 단위 실행) • 암호화 관리를 위한 TLS 보안 및 상호 인증 인터페이스 • Radius 인증 지원 • TACACS+AAA • SNMPv3 지원	
	• 2048비트 RSA 인증 • Elliptic Curve 인증	• Elliptic Curve 인증
인증	• CC(Common Criteria) NDcPP(Network Device Collaborative Protection Profile) • BSI(독일 연방 정보 보안청) • FIPS 140-2 Level 3 – 인증 #2379, #2635 • FIPS 197 – AES-256 – 인증 #2963, #2964, #3599, #3600 • IBM GDPS • EMC, Brocade	• CC(Common Criteria) NDcPP(Network Device Collaborative Protection Profile) • BSI(독일 연방 정보 보안청) • FIPS 140-2 Level 2 – 인증 #2697, #2843 • FIPS 197 – AES-256 – #3601, #3602, #4231, #4232, #5241 • IBM GDPS • EMC, Brocade

Ciena에 지금 연결하기